LOGICA Y TEORIA DE LA CIENCIA

LOGICA PARA MATEMATICOS

A. G. Hamilton

PARANINFO SA

LOGICA PARA MATEMATICOS

A. G. Hamilton

LOGICA PARA MATEMATICOS

1981

Colección:
LOGICA Y TEORIA DE LA CIENCIA

PARANINFO S.A.
MADRID

Traducido por
MARIO RODRIGUEZ ARTALEJO

© Cambridge University Press
© de la edición española, PARANINFO, S. A. Madrid (España)
© de la traducción, PARANINFO, S. A. Madrid (España)

Título original inglés:
LOGIC FOR MATHEMATICIANS

Reservados los derechos de edición,
reproducción o adaptación para todos
los países de lengua española

IMPRESO EN ESPAÑA
PRINTED IN SPAIN

ISBN: 0-521-29291-3 (edición inglesa)
ISBN: 84-283-1101-3 (edición española)

Depósito Legal: M-4560-1981

PARANINFO SA Magallanes, 25 - MADRID (15) (3-2831)

ALCO, artes gráficas. Jaspe, 34. Madrid-26

Indice

Prefacio 7

1. **Cálculo de enunciados informal** 9
   1.1. Enunciados y conectivas 9
   1.2. Funciones de verdad y tablas de verdad 12
   1.3. Reglas de manipulación y sustitución 19
   1.4. Formas normales 24
   1.5. Conjuntos adecuados de conectivas 28
   1.6. Argumentaciones y validez 31

2. **Cálculo de enunciados formal** 37
   2.1. El sistema formal L 37
   2.2. El Teorema de Adecuación para L 47

3. **Cálculo de predicados informal** 56
   3.1. Predicados y cuantificadores 56
   3.2. Lenguajes de primer orden 61
   3.3. Interpretaciones 68
   3.4. Satisfacción, verdad 71

4. **Cálculo de predicados formal** 84
   4.1. El sistema formal $K_{\mathscr{L}}$ 84
   4.2. Equivalencia, sustitución 92
   4.3. Forma prenexa 97
   4.4. El Teorema de Adecuación para K 103
   4.5. Modelos 111

5. **Sistemas matemáticos** 116
   5.1. Introducción 116
   5.2. Sistemas de primer orden con igualdad 117
   5.3. La teoría de grupos 123
   5.4. Aritmética de primer orden 128
   5.5. Teoría de conjuntos formal 132
   5.6. Consistencia y modelos 138

6. El Teorema de Incompletitud de Gödel 140
6.1. Introducción 140
6.2. Expresabilidad 142
6.3. Funciones y relaciones recursivas 149
6.4. Números de Gödel 158
6.5. La demostración de incompletitud 163

7. Computabilidad, insolubilidad, indecidibilidad 169
7.1. Algoritmo y computabilidad 169
7.2. Máquinas de Turing 178
7.3. Problemas de palabras 198
7.4. Indecibilidad de sistemas formales 204

Apéndice. Conjuntos numerables y no numerables 214

Indicaciones y soluciones de ejercicios seleccionados 219

Bibliografía 235

Glosario de símbolos 236

Indice alfabético 240

Prefacio

Todo matemático habrá sin duda experimentado cómo su respuesta a una pregunta de un no matemático sobre la naturaleza de su oficio tiene la virtud de detener la conversación. Para un lógico en compañía de otros matemáticos, el admitir su interrogación es dar lugar a análogas miradas en blanco, admisiones de ignorancia y un cambio del tópico de la conversación. La brecha entre los matemáticos y el público es una dificultad que siempre existirá (pese a que no debería perderse ninguna oportunidad de estrecharla), pero la brecha entre los lógicos y los otros matemáticos es, en mi opinión, innecesaria. Este libro es un intento de llenar el vacío proporcionando una introducción a la lógica para matemáticos que no aspiren necesariamente a convertirse en lógicos.

La lógica matemática se enseña actualmente en muchas universidades como parte de un curso de licenciatura en matemáticas o informática, y la materia es ya suficientemente coherente como para tener un cuerpo standard de temas fundamentales que deben incluirse en un primer curso introductorio. Este libro pretende ser un libro de texto para un tal curso, pero también pretende ser algo más: ser un libro, más bien que un mero libro de texto. El material se ha presentado deliberadamente de una manera directa, en razón de sí mismo, sin sesgos particulares hacia ningún aspecto, aplicación o desarrollo de la materia. Al mismo tiempo, se ha procurado situar el tema en el contexto de las matemáticas en su conjunto, y hacer énfasis en la relevancia de la lógica para el matemático.

El libro se ha diseñado de manera que sea accesible a cualquiera que disponga de una mínima base matemática, desde el estudiante de primer curso hasta el matemático profesional que quiere o tiene que hacerse una idea de lo que es la lógica matemática. Se supone una cierta familiaridad con el álgebra y la teoría de números elementales, y puesto que las ideas de conjunto numerable y no numerable son fundamentales, hay un apéndice en el que se describen las propiedades necesarias.

El material del libro se ha desarrollado a partir del presentado en dos cursos separados de dieciséis clases, impartidos en la Universidad de Stirling a estudiantes de los cursos tercero y cuarto de la licenciatura. El primero de estos cursos cubría los capítulos 1 a 4, junto con

algo del capítulo 5, y el segundo era un curso optativo más avanzado que cubría el resto. El capítulo 6 es el más difícil del libro, pero la importancia del Teorema de Incompletitud de Gödel es tal que las ideas que subyacen a su demostración habían de hacerse figurar en un libro como éste. Las demostraciones detalladas pueden omitirse en una primera lectura, puesto que el material del capítulo 7 no depende de ellas.

El alcance de este libro es más limitado que el de otras introducciones standard a la materia. En particular, la teoría de modelos y la teoría axiomática de conjuntos sólo se tocan de refilón. Por ello, referimos al lector interesado a la lista de títulos del final del libro para ulteriores lecturas. Algunos de estos títulos se citan expresamente en el libro (por el nombre del autor) y, en general, cubren la mayoría de las áreas de la lógica matemática y tratan con mayor profundidad los tópicos de este libro.

Hay ejercicios al final de cada sección. En general, los ejemplos rutinarios preceden a los que exigen mayor esfuerzo, pero todos los ejemplos pretenden ser aplicaciones directas del material de la correspondiente sección. Su propósito es clarificar y consolidar la materia, no extenderla. Al final del libro se proporcionan sugerencias o soluciones de muchos de los ejercicios.

Los símbolos en el libro son, en la medida de lo posible, standard (lo mismo que la terminología). No obstante, hay algunos usos no standard que se han introducido para aumentar la claridad. No causarán problemas al lector que esté familiarizado con la materia, y pretenden ayudar al que no lo esté. Es un hecho desafortunado el que diferentes autores usen diferentes notaciones y simbolismos. Por esta razón, y para facilitar las referencias, se ha incluido un glosario de símbolos. A lo largo de todo el texto, el símbolo $\triangleright$ se emplea para indicar la reasunción de la línea principal de exposición, después de haber sido rota ésta por una proposición, ejemplo, corolario o definición.

Finalmente, hay cuatro deudas que deseo reconocer. Primeramente, mi deuda para con el libro de Mendelson (*Introduction to Mathematical Logic*) será evidente para todos los que estén familiarizados con él. Como texto básico para lógicos tiene pocos rivales. En segundo lugar, este libro no hubiese sido posible sin el tiempo que puso a mi disposición la Universidad de Stirling. En tercer lugar, y a un nivel más personal, expreso mi mayor agradecimiento a Francis Bell por su concienzuda lectura de un borrador del texto y por sus numerosas y valiosas sugerencias. Y por último, vaya mi sincero agradecimiento a Irene Wilson y May Abrahamson por su paciente labor de mecanografía del manuscrito.

A. G. H.

1
Cálculo de enunciados informal

1.1 Enunciados y conectivas

La lógica, o al menos la matemática lógica, consiste en deducciones. Vamos a examinar las reglas de deducción haciendo uso de la precisión que caracteriza al enfoque matemático. Al hacer esto, si queremos que haya precisión tenemos que hacer inequívoco nuestro lenguaje, y la manera matemática standard de lograr esto consiste en introducir un lenguaje simbólico en el que los símbolos tengan significados y usos enunciados con toda precisión. Ante todo, examinaremos un aspecto del lenguaje cotidiano, a saber, las *conectivas* (o conjunciones[1], que es el término gramatical más común).

Cuando tratamos de analizar una frase en lenguaje castellano, observamos primeramente si se trata de una frase simple o de una frase compuesta. Una frase simple consta de un sujeto y un predicado (en el sentido gramatical). Por ejemplo:

Napoleón ha muerto

Juan le debe a Jaime doscientas pesetas

Todos los huevos que no son cuadrados son redondos

En cada caso, el sujeto se ha subrayado y la parte restante es el predicado. Una frase compuesta se forma a partir de frases simples por medio de conectivas. Por ejemplo:

Napoleón ha muerto y el mundo se regocija
Si todos los huevos no son cuadrados, entonces todos los huevos son redondos
Si el barómetro desciende, entonces lloverá o nevará

[1] La palabra «conjunción» tiene para nosotros un significado más específico. Se define en la sección 1.2.

Admitiremos como supuesto básico el que todas las frases simples que consideramos van a ser verdaderas o falsas. Ciertamente, podría argüirse que existen frases que no pueden considerarse ni verdaderas ni falsas, así que emplearemos otro término diferente: Nos referimos a *enunciados* simples y compuestos, y nuestro supuesto será que todos los enunciados son verdaderos o falsos.

Denotaremos los enunciados simples mediante letras mayúsculas A, B, C, ... Así, para simbolizar enunciados compuestos hemos de introducir símbolos para las conectivas. Las conectivas más comunes, y los símbolos que emplearemos para denotarlas, se indican en la tabla que sigue

no A	$\sim A$
A y B	$A \wedge B$
A o B	$A \vee B$
si A entonces B	$A \rightarrow B$
A si y sólo si B	$A \leftrightarrow B$

Naturalmente, si se ha de definir con precisión el significado de los símbolos, hemos de estar seguros de que conocemos con precisión el significado de las expresiones de la columna de la izquierda. Volveremos a esto en seguida.

Así pues, los tres enunciados compuestos vistos más arriba pueden escribirse simbólicamente:

$$A \wedge B$$
$$C \rightarrow D$$
$$E \rightarrow (F \vee G)$$

(respectivamente), donde A simboliza «Napoleón ha muerto», B simboliza «el mundo se regocija», C simboliza «todos los huevos no son cuadrados», etc.

Nótese que cuando un enunciado compuesto se simboliza de esta manera, lo que queda es el esqueleto lógico, una mera «forma enunciativa» que puede ser común a varios enunciados diferentes. Esto es precisamente lo que nos permite analizar las deducciones, ya que la deducción tiene que ver con las «formas» de los enunciados de una argumentación, más bien que con sus significados.

Ejemplo 1.1

Si Sócrates es un hombre entonces Sócrates es mortal
Sócrates es un hombre
$\therefore$ Sócrates es mortal

Esta es una argumentación que se considera lógicamente satisfactoria. Pero consideremos la argumentación:

Sócrates es un hombre
Sócrates es mortal

Puede pensarse que la conclusión se deduce de las premisas, pero esto es así a causa de los significados de las palabras «hombre» y «mortal», y no a causa de una deducción puramente lógica. Pongamos estas argumentaciones en forma simbólica.

$$\begin{array}{ll} A \rightarrow B & \qquad A \\ A & \therefore \quad B \\ \therefore \quad B & \end{array}$$

La «forma» de la primera es lo que la hace válida. Cualquier argumentación con la misma forma sería válida también. Esta es nuestra intuición lógica referente a enunciados del tipo si ... entonces ... No obstante, la segunda no comparte esta propiedad; hay muchas argumentaciones de esta forma que no consideraríamos válidas desde el punto de vista intuitivo. Por ejemplo:

La luna es amarilla
$\therefore$ La luna es de queso

Estudiaremos, pues, *formas enunciativas* más bien que enunciados particulares. Las letras *p*, *q*, *r*... serán *variables de enunciado* que designan enunciados simples arbitrarios no especificados. Nótese la distinción entre los usos de las letras *p*, *q*, *r*... y las letras *A*, *B*, *C*... Las primeras son variables que pueden ser sustituidas por enunciados simples particulares. Las últimas son meras «etiquetas» que designan ciertos enunciados simples particulares. Las variables nos permiten describir en un plano general las propiedades que poseen los enunciados y las conectivas. Ahora bien, todo enunciado simple es verdadero o falso, así que puede imaginarse que una variable de enunciado dada toma uno u otro de entre los dos *valores de verdad:* V (verdadero) o F (falso). El modo en que la verdad o falsedad de un enunciado compuesto o forma enunciativa compuesta depende de los valores de verdad de los enunciados simples o variables de enunciado que lo constituyen es el tema de la sección siguiente.

Ejercicios

1 Tradúzcanse a forma simbólica los siguientes enunciados compuestos:
(*a*) Si la demanda ha permanecido constante y los precios han aumentado, entonces el volumen de transacciones tiene que haber disminuido.

(*b*) Ganaremos las elecciones, suponiendo que a Ramírez se le elija como dirigente del partido.
(*c*) Si Ramírez no es elegido como dirigente del partido, entonces o González o Hernández dejarán el gabinete ministerial, y perderemos las elecciones.
(*d*) Si x es un número racional e y es un entero, entonces z no es real.
(*e*) O bien el asesino ha abandonado el país, o alguien está encubriéndole.
(*f*) Si el asesino no ha abandonado el país, entonces alguien está encubriéndole.
(*g*) La suma de dos números es par si y sólo si los dos números son pares o los dos números son impares.
(*h*) Si y es un entero entonces z no es real, supuesto que x sea un número racional.

2 (*a*) Escójanse pares de enunciados de la lista del ejercicio 1 que tengan la misma forma.
(*b*) Escójanse pares de enunciados de la lista del ejercicio 1 que tengan el mismo significado.

1.2 Funciones de verdad y tablas de verdad

Consideremos una por una las conectivas.

Negación

La negación de un enunciado A la escribimos como $\sim A$. Está claro que si A es verdadero entonces $\sim A$ es falso, y si A es falso entonces $\sim A$ es verdadero. El significado de A es irrelevante. Podemos describir la situación por medio de una *tabla de verdad:*

p	$\sim p$
V	F
F	V

La tabla indica el valor de verdad de $\sim p$ a partir del valor de verdad de p. La conectiva $\sim$ da lugar a una *función de verdad* $f^{\sim}$, que en este caso es una función del conjunto $\{V, F\}$ en sí mismo, definida por la tabla de verdad. Así pues:

$$f^{\sim}(V) = F$$
$$f^{\sim}(F) = V$$

Conjunción

Al igual que arriba, es fácil ver que el valor de verdad tomado por la conjunción $A \wedge B$ de dos enunciados A y B depende sólo del valor de

verdad tomado por A y del valor de verdad tomado por B. Se tiene la tabla:

p	q	$p \wedge q$
V	V	V
V	F	F
F	V	F
F	F	F

En la tabla tenemos una fila para cada una de las posibles combinaciones de valores de verdad para p y q. La última columna da los correspondientes valores de verdad para $p \wedge q$. La conectiva $\wedge$ define, pues, una función de verdad $f^{\wedge}$ de dos argumentos:

$$f^{\wedge}(V, V) = V$$
$$f^{\wedge}(V, F) = F$$
$$f^{\wedge}(F, V) = F$$
$$f^{\wedge}(F, F) = F$$

Disyunción

Hemos empleado $A \vee B$ para denotar «A o B», pero existen dos usos diferentes de la palabra «o» en castellano. «A o B» puede significar «A o B o ambos», o puede significar «A o B pero no ambos». A fin de mantener la precisión de nuestro lenguaje simbólico hemos de elegir solamente uno de éstos como significado de nuestro símbolo $\vee$. Escogemos el primero. No hay ninguna razón especial para hacerlo así; podríamos haber escogido igualmente el segundo. La tabla de verdad queda entonces:

p	q	$p \vee q$
V	V	V
V	F	V
F	V	V
F	F	F

La conectiva $\vee$ define una función de verdad de dos argumentos, de la misma manera que $\wedge$.

•

Observación: Si A y B son enunciados simples, podemos simbolizar «A o B pero no ambos» poniendo

$$(A \vee B) \wedge \sim(A \wedge B)$$

Análogamente, si hubiésemos usado «A o B pero no ambos» como definición del significado de nuestro símbolo de disyunción, podríamos haber expresado «A o B o ambos» usando la disyunción definida junto con $\wedge$ y $\sim$.

Condicional

$A \rightarrow B$ pretende representar el enunciado «A implica B» o «si A entonces B». Ahora bien, en este caso el uso normal del castellano no es de tanta ayuda a la hora de construir una tabla de verdad, y la tabla que vamos a utilizar es por lo general fuente de dificultades para la intuición. Es la siguiente:

p	q	$p \rightarrow q$
V	V	V
V	F	F
F	V	V
F	F	V

La dificultad radica en el valor de verdad V asignado a $A \rightarrow B$ en los casos en que A es falso. La consideración de ejemplos de enunciados condicionales en los cuales el antecedente es falso quizá pudiera llevarle a uno a la conclusión de que tales enunciados no poseen en absoluto un valor de verdad. Podría recibirse además la impresión de que esta clase de enunciados ni son útiles ni tienen sentido. Por ejemplo, del enunciado:

Si la hierba es roja entonces la luna es de queso

podría muy bien decirse que no tiene sentido.

No obstante, nosotros vamos a interesarnos por la deducción y los métodos de demostración, principalmente en matemáticas. En este contexto, el significado de un enunciado condicional $A \rightarrow B$ es que su veracidad permite inferir la veracidad de B a partir de la veracidad de A, y no permite inferir nada en particular a partir de la falsedad de A. Un tipo muy corriente de enunciado matemático puede servir para ilustrar esto. Se trata de los enunciados *universales*, por ejemplo:

Para todo entero n, si $n > 2$ entonces $n^2 > 4$

Esto se considera como un enunciado verdadero acerca de los enteros. Por lo tanto, cabe esperar que consideremos al enunciado

Si $n > 2$ entonces $n^2 > 4$

como verdadero, independientemente del valor que tome n. Diferentes valores de n dan lugar a todas las posibles combinaciones de valores de verdad para «$n > 2$» y «$n^2 > 4$», excepto la combinación VF. Tomando n como 3, -3, 1 respectivamente, resultan las combinaciones VV,

FV, *FF*, y éstas son las combinaciones que, de acuerdo con nuestra tabla, dan a la implicación el valor de verdad *V*. La veracidad intuitiva de la implicación que hemos considerado sirve pues en cierta medida de justificación a la tabla de verdad. El punto a recordar es que la única circunstancia en la que el enunciado $A \rightarrow B$ se considera falso es cuando A es verdadero y B es falso.

Bicondicional

Denotaremos «A si y sólo si B» por $A \leftrightarrow B$. Aquí la situación es clara: $A \leftrightarrow B$ deberá ser verdadero cuando A y B tengan el mismo valor de verdad (ambos verdaderos o ambos falsos) y sólo entonces. La tabla de verdad es entonces:

p	q	$p \leftrightarrow q$
V	V	V
V	F	F
F	V	F
F	F	V

Esto completa nuestra lista de conectivas. Es obvio que utilizando estas conectivas se pueden construir enunciados compuestos de cualquier longitud a partir de enunciados simples. Usando variables de enunciados podemos construir *formas* enunciativas de cualquier longitud.

Definición 1.2

Una *forma enunciativa* es una expresión en la que intervienen variables de enunciado y conectivas, que pueda formarse utilizando las reglas:

(i) Toda variable de enunciado es una forma enunciativa.

(ii) Si $\mathscr{A}$ y $\mathscr{B}$ son formas enunciativas, entonces $(\sim \mathscr{A})$, $(\mathscr{A} \wedge \mathscr{B})$, $(\mathscr{A} \vee \mathscr{B})$, $(\mathscr{A} \rightarrow \mathscr{B})$ y $(\mathscr{A} \leftrightarrow \mathscr{B})$ son formas enunciativas.

Ejemplo 1.3

$((p \wedge q) \rightarrow (\sim (q \vee r)))$ es una forma enunciativa. Por (i), p, q, r son formas enunciativas. Por (ii), $(p \wedge q)$ y $(q \vee r)$ son formas enunciativas. Por (ii), $(\sim (q \vee r))$ es una forma enunciativa. Por (ii), $((p \wedge q) \rightarrow (\sim (q \vee r)))$ es una forma enunciativa.

▷ Esta definición es un ejemplo de definición inductiva. Establece un patrón que volverá a aparecer de nuevo cuando describamos en detalle los sistemas formales.

Las conectivas determinan funciones de verdad simples. Usando las tablas de verdad de las conectivas, podemos construir una tabla de verdad para cualquier forma enunciativa dada. Nos referimos a una tabla que indique, para cualquier asignación dada de valores de ver-

dad a las variables de enunciado que aparezcan en la forma enunciativa, el valor de verdad que tome ésta. Esta tabla de verdad es una representación gráfica de una función de verdad. Así pues, toda forma enunciativa da lugar a una función de verdad, cuyo número de argumentos es igual al número de variables de enunciado distintas que aparezcan en la forma enunciativa. Ilustremos esto mediante algunos ejemplos.

Ejemplo 1.4

(*a*) $((\sim p) \vee q)$.

Primeramente se construye la tabla de verdad:

p	q	$(\sim p)$	$((\sim p) \vee q)$
V	*V*	*F*	*V*
V	*F*	*F*	*F*
F	*V*	*V*	*V*
F	*F*	*V*	*V*

Obsérvese que la función de verdad correspondiente a esta forma enunciativa es la misma que la función de verdad determinada por $(p \rightarrow q)$.

(*b*) $(p \rightarrow (q \vee r))$.

Tabla de verdad:

p	q	r	$(q \vee r)$	$(p \rightarrow (q \vee r))$
V	*V*	*V*	*V*	*V*
V	*V*	*F*	*V*	*V*
V	*F*	*V*	*V*	*V*
V	*F*	*F*	*F*	*F*
F	*V*	*V*	*V*	*V*
F	*V*	*F*	*V*	*V*
F	*F*	*V*	*V*	*V*
F	*F*	*F*	*F*	*V*

La función de verdad tiene en este caso tres argumentos, puesto que hay tres variables de enunciado. Cada fila de la tabla da el valor de la función de verdad para una combinación diferente de valores de verdad para las letras. Nótese que la tabla de verdad de cualquier forma enunciativa en la que intervengan tres variables de enunciado tendrá ocho filas, y obsérvese el patrón según el cual se han escrito las tres primeras columnas de la tabla. Esta manera de agrupar las *V*s y

*F*s bajo las letras *p*, *q*, *r* asegura que cada posible combinación aparezca una vez y sólo una.

▷ En el caso general, a una forma enunciativa en la que intervengan n variables de enunciado diferente (siendo n cualquier número natural) le corresponderá una función de verdad de n argumentos, y la tabla de verdad tendrá 2^n filas, una para cada una de las posibles combinaciones de valores de verdad para las variables de enunciado. Nótese además que existen 2^{2^n} funciones de verdad distintas de n argumentos, que corresponden a las 2^{2^n} maneras posibles de disponer las *V*s y las *F*s en la última columna de una tabla de verdad de 2^n filas. Está claro que el número de formas enunciativas que se pueden construir utilizando n variables de enunciado es infinito, así que formas enunciativas distintas pueden corresponder a una misma función de verdad.

Para investigar esto más a fondo necesitamos algunas definiciones.

Definición 1.5

(*a*) Una forma enunciativa es una *tautología* si toma el valor de verdad *V* bajo cada una de las posibles asignaciones de valores de verdad a las variables de enunciado que aparecen en ella.

(*b*) Una forma enunciativa es una *contradicción* si toma el valor de verdad *F* bajo cada una de las posibles asignaciones de valores de verdad a las variables de enunciado que aparecen en ella.

▷ No toda forma enunciativa cae en una u otra de estas categorías. De hecho, ninguna de las consideradas hasta aquí cae en ellas.

Ejemplo 1.6

(*a*) $(p \vee (\sim p))$ es una tautología.
(*b*) $(p \wedge (\sim p))$ es una contradicción.
(*c*) $(p \leftrightarrow (\sim(\sim p)))$ es una tautología.
(*d*) $(((\sim p) \rightarrow q) \rightarrow (((\sim p) \rightarrow (\sim q)) \rightarrow p))$ es una tautología.

El método que se utiliza para comprobar si una forma enunciativa dada es una tautología o una contradicción consiste en construir la tabla de verdad.

▷ Debería resultar claro a partir de la definición que todas las tautologías que contengan n variables de enunciado dan lugar a una misma función de verdad de n argumentos, concretamente la que toma siempre el valor *V*. Con respecto a las contradicciones puede hacerse una observación similar.

Definición 1.7

Si $\mathscr{A}$ y $\mathscr{B}$ son formas enunciativas, diremos que $\mathscr{A}$ *implica lógicamente* a $\mathscr{B}$ si $(\mathscr{A}\rightarrow\mathscr{B})$ es una tautología, y que $\mathscr{A}$ es *lógicamente equivalente* a $\mathscr{B}$ si $(\mathscr{A}\leftrightarrow\mathscr{B})$ es una tautología.

Ejemplo 1.8

(*a*) $(p \wedge q)$ implica lógicamente a p.
(*b*) $(\sim(p \wedge q))$ es lógicamente equivalente a $((\sim p) \vee (\sim q))$.
(*c*) $(\sim(p \vee q))$ es lógicamente equivalente a $((\sim p) \wedge (\sim q))$.

Ad (*a*): Tabla de verdad de $((p \wedge q)\rightarrow p)$:

$((p$	$\wedge$	$q)$	$\rightarrow$	$p)$
V	V	V	V	V
V	F	F	V	V
F	F	V	V	F
F	F	F	V	F

Ad (*b*):

$(\sim$	$(p$	$\wedge$	$q)$	$\leftrightarrow$	$((\sim$	$p)$	$\vee$	$(\sim$	$q)))$
F	V	V	V	V	F	V	F	F	V
V	V	F	F	V	F	V	V	V	F
V	F	F	V	V	V	F	V	F	V
V	F	F	F	V	V	F	V	V	F

Aquí hemos introducido otra manera de escribir tablas de verdad. Para formas enunciativas complicadas es más fácil escribir la tabla de este modo. Se empieza escribiendo columnas de Vs y Fs debajo de las variables de enunciado en el mismo orden que ya conocemos de tablas anteriores, para asegurarnos de que cada combinación aparezca una sola vez. Esto se ha de hacer, por supuesto, de manera consistente a lo largo de todas las intervenciones de una misma variable. Seguidamente, se van insertando bajo las conectivas los valores de verdad de las diversas partes, hasta llegar a rellenar la columna correspondiente a la forma enunciativa completa. En los ejemplos de más arriba, dicha columna está enmarcada por líneas verticales.

Observación: Sean $\mathscr{A}$ y $\mathscr{B}$ formas enunciativas que contengan las mismas variables de enunciado. Si $\mathscr{A}$ y $\mathscr{B}$ son lógicamente equivalentes, entonces representan una misma función de verdad. Puesto que si $(\mathscr{A}\leftrightarrow\mathscr{B})$ es una tautología, no toma nunca el valor F, de modo que $\mathscr{A}$ y $\mathscr{B}$ han de tomar siempre el mismo valor de verdad. Así pues, las funciones de verdad correspondientes a $\mathscr{A}$ y $\mathscr{B}$ han de ser forzosamente iguales.

Ejercicios

3 Escríbanse las tablas de verdad de las siguientes formas enunciativas:

(*a*) $((\sim p) \wedge (\sim q))$;
(*b*) $\sim((p \rightarrow q) \rightarrow (\sim(q \rightarrow p)))$;
(*c*) $(p \rightarrow (q \rightarrow r))$;
(*d*) $((p \wedge q) \rightarrow r)$;
(*e*) $((p \leftrightarrow (\sim q)) \vee q)$;
(*f*) $((p \wedge q) \vee (r \wedge s))$;
(*g*) $(((\sim p) \wedge q) \rightarrow ((\sim q) \wedge r))$;
(*h*) $((p \rightarrow (q \rightarrow r)) \rightarrow ((p \rightarrow q) \rightarrow (p \rightarrow r)))$.

4 Demuéstrese que la forma enunciativa $((\sim p) \vee q)$ da lugar a la misma función de verdad que $(p \rightarrow q)$, y que $((\sim p) \rightarrow (q \vee r))$ da lugar a la misma función de verdad que $((\sim q) \rightarrow ((\sim r) \rightarrow p))$.

5 ¿Cuáles de entre las siguientes formas enunciativas son tautologías?

(*a*) $(p \rightarrow (q \rightarrow p))$;
(*b*) $((q \vee r) \rightarrow ((\sim r) \rightarrow q))$;
(*c*) $((p \wedge (\sim q)) \vee ((q \wedge (\sim r)) \vee (r \wedge (\sim p))))$;
(*d*) $((p \rightarrow (q \rightarrow r)) \rightarrow ((p \wedge (\sim q)) \vee r))$.

6 Demuéstrese que los siguientes pares de formas enunciativas son lógicamente equivalentes.

(*a*) $(p \rightarrow q)$, $((\sim q) \rightarrow (\sim p))$;
(*b*) $((p \vee q) \wedge r)$, $((p \wedge r) \vee (q \wedge r))$;
(*c*) $(((\sim p) \wedge (\sim q)) \rightarrow (\sim r))$, $(r \rightarrow (q \wedge p))$;
(*d*) $(((\sim p) \vee q) \rightarrow r)$, $((p \wedge (\sim q)) \vee r)$.

7 Demuéstrese que la forma enunciativa $(((\sim p) \rightarrow q) \rightarrow (p \rightarrow (\sim q)))$ no es una tautología. Encuéntrense formas enunciativas $\mathscr{A}$ y $\mathscr{B}$ tales que $(((\sim \mathscr{A}) \rightarrow \mathscr{B}) \rightarrow (\mathscr{A} \rightarrow (\sim \mathscr{B})))$ sea una contradicción.

1.3 Reglas de manipulación y sustitución

Proposición 1.9

Si $\mathscr{A}$ y $(\mathscr{A} \rightarrow \mathscr{B})$ son tautologías, entonces $\mathscr{B}$ es una tautología.
Demostración: Supongamos que $\mathscr{A}$ y $(\mathscr{A} \rightarrow \mathscr{B})$ son tautologías y que $\mathscr{B}$ no lo es. Entonces existe una asignación de valores de verdad a las variables de enunciado que aparecen en $\mathscr{A}$ o en $\mathscr{B}$, que da a $\mathscr{B}$ el valor *F*. Pero esta asignación debe dar a $\mathscr{A}$ el valor *V*, ya que $\mathscr{A}$ es una tautología, y por tanto da a $(\mathscr{A} \rightarrow \mathscr{B})$ el valor *F*. Esto contradice la hipótesis de que $(\mathscr{A} \rightarrow \mathscr{B})$ es una tautología. Así pues, $\mathscr{B}$ debe ser una tautología.

▷ Consideremos la forma enunciativa $(p \rightarrow p)$. Es fácil demostrar que es

una tautología. Ahora bien, si sustituimos p por la forma enunciativa $((r \wedge s) \rightarrow t)$ en ambos lugares, obtenemos

$$(((r \wedge s) \rightarrow t) \rightarrow ((r \wedge s) \rightarrow t)$$

que vuelve a ser una tautología. Intuitivamente, está claro que esto mismo ocurriría sea cual sea la forma enunciativa que sustituyésemos en el lugar de p, siempre que sustituyésemos en *todas* las intervenciones de p. (La forma enunciativa $(p \rightarrow ((r \wedge s) \rightarrow t))$ obviamente no es tautología). Recogemos esta idea en una proposición.

Proposición 1.10

Sea $\mathscr{A}$ una forma enunciativa en la que aparecen las variables de enunciado $p_1, p_2, \ldots, p_n$, y sean $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ formas enunciativas cualesquiera. Si $\mathscr{A}$ es una tautología entonces la forma enunciativa $\mathscr{B}$, obtenida a partir de $\mathscr{A}$ reemplazando cada intervención de p_i por $\mathscr{A}_i$ $(1 \leqslant i \leqslant n)$, es también una tautología.

Demostración: Sea $\mathscr{A}$ una tautología y sean $p_1, p_2, \ldots, p_n$ las variables de enunciado que aparecen en $\mathscr{A}$. Sean $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ formas enunciativas cualesquiera. Asignemos valores de verdad arbitrarios a las variables de enunciado que aparecen en $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$. El valor de verdad que toma $\mathscr{B}$ es el mismo que habría tomado $\mathscr{A}$ si los valores tomados por $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ se hubiesen asignado a $p_1, p_2, \ldots, p_n$, respectivamente; es decir, V. Así pues, $\mathscr{B}$ toma el valor V bajo cualquier asignación de valores de verdad; es decir, $\mathscr{B}$ es una tautología.

$\triangleright$ La proposición 1.10 es una de entre varias que nos iremos encontrando, cuyas aplicaciones están muy extendidas y son muy a menudo inconscientes. Por ejemplo, la siguiente proposición es un resultado útil.

Proposición 1.11

Cualesquiera que sean las formas enunciativas $\mathscr{A}$ y $\mathscr{B}$, $(\sim(\mathscr{A} \wedge \mathscr{B}))$ es lógicamente equivalente a $((\sim\mathscr{A}) \vee (\sim\mathscr{B}))$ y $(\sim(\mathscr{A} \vee \mathscr{B}))$ es lógicamente equivalente a $((\sim\mathscr{A}) \wedge (\sim\mathscr{B}))$.

Demostración: Vimos antes que

$$(\sim(p \wedge q) \leftrightarrow ((\sim p) \vee (\sim q))$$

es una tautología. De la proposición 1.10 se deduce que para formas enunciativas cualesquiera $\mathscr{A}$ y $\mathscr{B}$,

$$((\sim(\mathscr{A} \wedge \mathscr{B})) \leftrightarrow ((\sim\mathscr{A}) \vee (\sim\mathscr{B})))$$

es también una tautología. Por tanto, $(\sim(\mathscr{A} \wedge \mathscr{B}))$ es lógicamente equivalente a $((\sim\mathscr{A}) \vee (\sim\mathscr{B}))$. La otra parte se demuestra análogamente.

Ejemplo 1.12

Para formas enunciativas cualesquiera $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$, $(\mathscr{A} \wedge (\mathscr{B} \wedge \mathscr{C}))$ es lógicamente equivalente a $((\mathscr{A} \wedge \mathscr{B}) \wedge \mathscr{C})$. (A causa de esto, se acostumbra a omitir los paréntesis interiores y escribir $(\mathscr{A} \wedge \mathscr{B} \wedge \mathscr{C})$.)

Consideremos la forma enunciativa

$$(((p_1 \wedge (p_2 \wedge p_3)) \leftrightarrow ((p_1 \wedge p_2) \wedge p_3)))$$

Construyendo una tabla de verdad de la manera usual, puede demostrarse que es una tautología. Aplicando ahora la proposición 1.10, sustituyendo $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ en el lugar de p_1, p_2, p_3, se obtiene el resultado deseado.

Ejemplo 1.13

Para formas enunciativas cualesquiera $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$, los siguientes pares de formas enunciativas son lógicamente equivalentes.

(*a*) $(\mathscr{A} \vee (\mathscr{B} \vee \mathscr{C}))$ y $((\mathscr{A} \vee \mathscr{B}) \vee \mathscr{C})$
(*b*) $(\mathscr{A} \wedge \mathscr{B})$ y $(\mathscr{B} \wedge \mathscr{A})$
(*c*) $(\mathscr{A} \vee \mathscr{B})$ y $(\mathscr{B} \vee \mathscr{A})$

Para verificarlo, se sigue el patrón del ejemplo anterior.

▷ Consideremos ahora la forma enunciativa $((p \wedge p) \rightarrow q)$. $(p \wedge p)$, que aparece en ella, es lógicamente equivalente a p (ya que $((p \wedge p) \leftrightarrow p)$ es una tautología). Reemplazando $(p \wedge p)$ por p, obtenemos $(p \rightarrow q)$. Ahora bien, $(p \rightarrow q)$ es lógicamente equivalente a $((p \wedge p) \rightarrow q)$ (compruébese mediante tabla de verdad). De nuevo se trata de un caso particular de una proposición general sobre sustitución.

Proposición 1.14

Si $\mathscr{B}_1$ es una forma enunciativa resultante de sustituir en la forma enunciativa $\mathscr{A}_1$ una o más intervenciones de la forma enunciativa $\mathscr{B}$ por la forma enunciativa $\mathscr{A}$, y si $\mathscr{B}$ es lógicamente equivalente a $\mathscr{A}$, entonces $\mathscr{B}_1$ es lógicamente equivalente a $\mathscr{A}_1$.

Demostración: Supongamos que $\mathscr{B}$ es lógicamente equivalente a $\mathscr{A}$ y que $\mathscr{B}_1$ y $\mathscr{A}_1$ son como se ha descrito. Queremos demostrar que $(\mathscr{A}_1 \leftrightarrow \mathscr{B}_1)$ es una tautología. Asignemos valores de verdad a todas las variables de enunciado que intervienen. $\mathscr{B}_1$ se diferencia de $\mathscr{A}_1$ tan sólo en que en algunos lugares $\mathscr{B}$ está donde antes estaba $\mathscr{A}$. El valor de verdad tomado por $\mathscr{B}_1$ tiene que ser el mismo que tome $\mathscr{A}_1$, ya que $\mathscr{A}$ y $\mathscr{B}$ tienen el mismo valor de verdad. Así pues, $(\mathscr{A}_1 \leftrightarrow \mathscr{B}_1)$ toma el valor *V*. Se deduce que $(\mathscr{A}_1 \leftrightarrow \mathscr{B}_1)$ toma siempre el valor *V*, ya que los valores de verdad asignados originalmente a las variables eran arbitra-

rios. Así pues, $(\mathscr{A}_1 \leftrightarrow \mathscr{B}_1)$ es una tautología y $\mathscr{A}_1$ es lógicamente equivalente a $\mathscr{B}_1$.

▷La proposición siguiente no es parte integrante del desarrollo, pero la incluimos aquí porque da una impresión de los métodos que utilizaremos más adelante. Por esta razón trataremos con algún detalle la demostración.

Proposición 1.15

Llamemos forma enunciativa restringida a una forma enunciativa en la que solamente figuren las conectivas $\sim$, $\wedge$ y $\vee$. Sea $\mathscr{A}$ una forma enunciativa restringida, y supongamos que $\mathscr{A}^*$ se ha obtenido a partir de $\mathscr{A}$ intercambiando $\wedge$ y $\vee$ y reemplazando cada variable de enunciado por su negación. Entonces $\mathscr{A}^*$ es lógicamente equivalente a $(\sim\mathscr{A})$.

Demostración: La demostración procede por inducción sobre el número n de conectivas que aparecen en $\mathscr{A}$. Si logramos demostrar que, para cada número natural n, toda forma enunciativa restringida $\mathscr{A}$ que tenga exactamente n conectivas satisface la proposición, está claro que habremos demostrado todo lo necesario.

Paso base: $n=0$ ($\mathscr{A}$ no contiene conectivas). En este caso $\mathscr{A}$ consiste simplemente en una variable de enunciado, p, por ejemplo. Así, $\mathscr{A}^*$ es en este caso $(\sim p)$, de modo que, trivialmente, $\mathscr{A}^*$ es lógicamente equivalente a $(\sim\mathscr{A})$.

Paso de inducción: Supongamos que $n>0$, que $\mathscr{A}$ tiene n conectivas, y que toda forma enunciativa con menos de n conectivas posee la propiedad requerida. Debido a las tres maneras de construir formas enunciativas, hemos de considerar tres casos:

Caso 1: $\mathscr{A}$ es de la forma $(\sim\mathscr{B})$.
Caso 2: $\mathscr{A}$ es de la forma $(\mathscr{B} \vee \mathscr{C})$.
Caso 3: $\mathscr{A}$ es de la forma $(\mathscr{B} \wedge \mathscr{C})$.

Ad Caso 1: $\mathscr{B}$ tiene $n-1$ conectivas, así que por hipótesis de inducción $\mathscr{B}^*$ es lógicamente equivalente a $(\sim\mathscr{B})$. Pero $\mathscr{A}^*$ es $(\sim\mathscr{B}^*)$, así que $\mathscr{A}^*$ es lógicamente equivalente a $(\sim(\sim\mathscr{B}))$, por ejemplo, a $(\sim\mathscr{A})$. Nótese que, casi inconscientemente, hemos usado aquí el resultado de la proposición 1.14.

Ad Caso 2: $\mathscr{B}$ y $\mathscr{C}$ contienen cada una menos de n conectivas, así que $\mathscr{B}^*$ y $\mathscr{C}^*$ son lógicamente equivalentes a $(\sim\mathscr{B})$ y $(\sim\mathscr{C})$, respectivamente. Ahora bien, $\mathscr{A}^*$ es $(\mathscr{B}^* \wedge \mathscr{C}^*)$. Por la proposición 1.14 esto es

lógicamente equivalente a $((\sim\mathscr{B}) \wedge \mathscr{C}^*)$, y de nuevo por la misma proposición, esto es lógicamente equivalente a $((\sim\mathscr{B}) \wedge (\sim\mathscr{C}))$. Ahora bien, hemos visto ya (proposición 1.11) que esto es equivalente a $(\sim(\mathscr{B} \vee \mathscr{C}))$, es decir, $(\sim\mathscr{A})$. Así pues, $\mathscr{A}^*$ es lógicamente equivalente a $(\sim\mathscr{A})$.

Ad Caso 3: Como en el Caso 2, $\mathscr{B}^*$ y $\mathscr{C}^*$ son lógicamente equivalentes a $(\sim\mathscr{B})$ y $(\sim\mathscr{C})$, respectivamente. $\mathscr{A}^*$ es $(\mathscr{B}^* \vee \mathscr{C}^*)$, que es lógicamente equivalente a $((\sim\mathscr{B}) \vee \mathscr{C}^*)$ y por tanto a $((\sim\mathscr{B}) \vee (\sim\mathscr{C}))$ y por tanto a $(\sim(\mathscr{B} \wedge \mathscr{C}))$, es decir, a $(\sim\mathscr{A})$. Así pues, $\mathscr{A}^*$ es lógicamente equivalente a $(\sim\mathscr{A})$.

Bajo la hipótesis de que toda forma enunciativa restringida con menos de n consecutivas posee la propiedad requerida, hemos demostrado que toda forma enunciativa restringida con n conectivas posee la propiedad requerida. Así pues, por el principio de inducción matemática, toda forma enunciativa restringida tiene la propiedad requerida.

Corolario 1.16

Si $p_1, p_2, \ldots, p_n$ son variables de enunciado, entonces

$$((\sim p_1) \vee (\sim p_2) \vee \ldots \vee (\sim p_n))$$

es lógicamente equivalente a

$$(\sim(p_1 \wedge \ldots \wedge p_n))$$

Demostración: Este es un caso especial de la proposición 1.15, en el que es la forma enunciativa $(p_1 \wedge p_2 \wedge \ldots \wedge p_n)$.

▷ Introduciendo una nueva notación con el fin de abreviar, podemos escribir este resultado poniendo

$$\left(\bigvee_{i=1}^{n} (\sim p_i)\right) \text{ es lógicamente equivalente a } \left(\sim\left(\bigwedge_{i=1}^{n} p_i\right)\right)$$

También podemos usar la proposición para demostrar el resultado «dual» del anterior, a saber

$$((\sim p_1) \wedge (\sim p_2) \wedge \ldots \wedge (\sim p_n))$$

es lógicamente equivalente a

$$(\sim(p_1 \vee p_2 \vee \ldots \vee p_n)),$$

es decir, $\left(\bigwedge_{i=1}^{n} (\sim p_i)\right)$ es lógicamente equivalente a $\left(\sim\left(\bigvee_{i=1}^{n} p_i\right)\right)$

Proposición 1.17 (leyes de De Morgan)

Sean $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ formas enunciativas cualesquiera. Entonces:

(i) $(\bigvee_{i=1}^{n}(\sim\mathscr{A}_i))$ es lógicamente equivalente a $(\sim(\bigwedge_{i=1}^{n}\mathscr{A}_i))$
(ii) $((\bigwedge_{i=1}^{n}(\sim\mathscr{A}_i))$ es lógicamente equivalente a $(\sim(\bigvee_{i=1}^{n}\mathscr{A}_i))$

Demostración: Usando los corolarios anteriores y la proposición 1.10.

Ejercicios

8 Demuéstrese que, para formas enunciativas cualesquiera $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$, los siguientes pares de formas enunciativas son lógicamente equivalentes.

(*a*) $(\mathscr{A} \vee (\mathscr{B} \vee \mathscr{C}))$ y $((\mathscr{A} \vee \mathscr{B}) \vee \mathscr{C})$;
(*b*) $(\mathscr{A} \wedge \mathscr{B})$ y $(\mathscr{B} \wedge \mathscr{A})$;
(*c*) $(\mathscr{A} \vee \mathscr{B})$ y $(\mathscr{B} \vee \mathscr{A})$;
(*d*) $\mathscr{A}$ y $(\sim(\sim\mathscr{A}))$.

9 Demuéstrese que, para formas enunciativas cualesquiera $\mathscr{A}$ y $\mathscr{B}$, las siguientes formas enunciativas son tautologías.

(*a*) $((\mathscr{A} \wedge \mathscr{B})\rightarrow\mathscr{A})$;
(*b*) $((\mathscr{A} \wedge \mathscr{B}))\rightarrow\mathscr{B})$;

10 Demuéstrese, usando la proposición 1.14, que $((\sim((\sim p) \vee q)) \vee r)$ es lógicamente equivalente a $((p\rightarrow q)\rightarrow r)$.

11 Demuéstrese, usando las proposiciones 1.14 y 1.17, que la forma enunciativa $((\sim(p \vee (\sim q)))\rightarrow(q\rightarrow r))$ es lógicamente equivalente a cada una de las siguientes.

(*a*) $((\sim(q\rightarrow p))\rightarrow((\sim q) \vee r))$;
(*b*) $(((\sim p) \wedge q)\rightarrow(\sim(q \wedge (\sim r))))$;
(*c*) $((\sim((\sim q) \vee r))\rightarrow(q\rightarrow p))$;
(*d*) $(q\rightarrow(p \vee r))$.

1.4 Formas normales

Sigamos considerando lo que hemos llamado formas enunciativas restringidas. Hemos observado antes que a partir de toda forma enunciativa puede construirse una tabla de verdad. Vamos a demostrar ahora un resultado recíproco.

Proposición 1.18

Toda función de verdad es la función de verdad determinada por una forma enunciativa tal que todas las conectivas que figuran en ella están entre $\sim$, $\wedge$ y $\vee$ (es decir, una forma enunciativa restringida).

Demostración: Supongamos que la función dada es de n argumentos Vamos a construir una forma enunciativa $\mathscr{A}$ a partir de las variables $p_1, p_2, \ldots, p_n$. Observemos primeramente que si la función de verdad toma el valor F para toda combinación de valores de verdad, entonces corresponde a cualquier contradicción, y la forma enunciativa

$$((p_1 \wedge (\sim p_1)) \wedge p_2 \wedge p_3 \ldots \wedge p_n)$$

nos servirá.

Supongamos ahora que la función de verdad toma el valor V por lo menos una vez. Nuestro método se basa en construir, para cada una de las 2^n combinaciones de valores de verdad, una forma enunciativa que sea verdadera para esa combinación y falsa para todas las demás combinaciones. Por ejemplo, si $n=3$, la forma enunciativa $(p_1 \wedge (\sim p_2) \wedge (\sim p_3))$ es verdadera solamente para la combinación VFF de valores de verdad para p_1, p_2, p_3 respectivamente, y $((\sim p_1) \wedge (\sim p_2) \wedge p_3)$ es verdadera solamente para la combinación FFV. Estas formas enunciativas especiales se llaman *conjunciones básicas*. Dada una asignación de valores de verdad a $p_1, p_2, \ldots, p_n$, ponemos p_i en la conjunción si a p_i se le asigna V, y ponemos $(\sim p_i)$ en la conjunción si a p_i se le asigna F, para $1 \leqslant i \leqslant n$. Entonces, para la asignación de valores de verdad dada, todos los miembros de la conjunción tienen el valor V, y así la conjunción completa recibe el valor V. De análoga manera, para cualquier otra asignación de valores de verdad, al menos uno de los miembros de la conjunción recibirá el valor F, de modo que la conjunción total tomará el valor F.

Para demostrar ahora nuestra proposición, consideremos todas las combinaciones de n valores de verdad para las cuales nuestra función de verdad arroja el valor V. Sea $\mathscr{A}$ la disyunción de todas las conjunciones básicas obtenidas tomando estas combinaciones como los valores de verdad de $p_1, p_2, \ldots p_n$. Esta $\mathscr{A}$ es la forma enunciativa requerida. Para convencernos de ello, asignemos valores de verdad a $p_1, p_2, \ldots, p_n$. Si nuestra función de verdad aplicada a esta combinación arroja el valor V, entonces la correspondiente conjunción básica está en $\mathscr{A}$ y toma el valor V para la asignación de valores de verdad en cuestión, así que $\mathscr{A}$ toma asimismo el valor V. Si nuestra función de verdad aplicada a esta combinación arroja el valor F, entonces la correspondiente conjunción básica no está incluida en $\mathscr{A}$, y todas las demás conjunciones básicas incluidas en $\mathscr{A}$ toman el valor F para la asignación de valores de verdad en cuestión, con lo cual $\mathscr{A}$ toma también el valor F. Así pues, para cualquier asignación de valores de verdad, el valor de verdad de $\mathscr{A}$ es el dado por la función de verdad.

Para entender mejor esta demostración conviene referirla a un ejemplo concreto.

Ejemplo 1.19

Especifiquemos una función de verdad por medio de una tabla (se trata de una función de tres argumentos).

V	*V*	*V*	*V*
V	*V*	*F*	*V*
V	*F*	*V*	*F*
V	*F*	*F*	*F*
F	*V*	*V*	*F*
F	*V*	*F*	*F*
F	*F*	*V*	*F*
F	*F*	*F*	*V*

Las combinaciones de valores de verdad para las que la función arroja el valor *V* son *VVV*, *VVF* y *FFF*. Las conjunciones básicas correspondientes son:

$$(p_1 \wedge p_2 \wedge p_3)$$
$$(p_1 \wedge p_2 \wedge (\sim p_3))$$
$$((\sim p_1) \wedge (\sim p_2) \wedge (\sim p_3))$$

La forma enunciativa $\mathscr{A}$ construida en la demostración es

$$(p_1 \wedge p_2 \wedge p_3) \vee (p_1 \wedge p_2 \wedge (\sim p_3)) \vee ((\sim p_1) \wedge (\sim p_2) \wedge (\sim p_3))$$

Esta forma enunciativa corresponde a la función de verdad dada, y la tabla dada es su tabla de verdad.

Corolario 1.20

Toda forma enunciativa que no sea contradicción es lógicamente equivalente a una forma enunciativa restringida de la forma

$$(\bigvee_{i=1}^{m} (\bigwedge_{j=1}^{n} Q_{ij})),$$

siendo Q_{ij} una variable de enunciado o la negación de una variable de enunciado. Esta forma se llama *forma normal disyuntiva.*

Demostración: Dos formas enunciativas son lógicamente equivalentes si y sólo si corresponden a la misma función de verdad. Dada una forma enunciativa $\mathscr{A}$, obtenemos su tabla de verdad y la función de verdad que ésta define. Aplicamos entonces el método de la proposición 1.18 para obtener una forma enunciativa en la forma deseada, correspondiente a dicha función de verdad.

Corolario 1.21

Toda forma enunciativa que no sea tautología es lógicamente equivalente a una forma enunciativa restringida de la forma

$$(\bigwedge_{i=1}^{m} (\bigvee_{j=1}^{n} Q_{ij})),$$

siendo cada Q_{ij} una variable de enunciado o la negación de una variable de enunciado. Esta forma se llama *forma normal conjuntiva.*

Demostración: Sea $\mathscr{A}$ una forma enunciativa que no es tautología. Entonces $\sim\mathscr{A}$ no es contradicción y es lógicamente equivalente a una forma enunciativa $(\vee_{i=1}^{m}(\wedge_{j=1}^{n} Q_{ij}))$ en forma normal conjuntiva. $\mathscr{A}$ es pues lógicamente equivalente a $(\sim(\vee_{i=1}^{m}(\wedge_{j=1}^{n} Q_{ij})))$, y por las leyes de De Morgan, esto es lógicamente equivalente a $(\wedge_{i=1}^{m}(\vee_{j=1}^{n}(\sim Q_{ij})))$. El resultado se deduce reemplazando en esta forma enunciativa cada expresión de la forma $(\sim(\sim q))$ por q.

Ejemplo 1.22

Encuéntrese una forma normal conjuntiva lógicamente equivalente a

$$(((\sim p_1) \vee p_2) \rightarrow p_3)$$

Construimos una forma normal conjuntiva lógicamente equivalente a

$\sim$	$(((\sim$	$p_1)$	$\vee$	$p_2)$	$\rightarrow$	$p_3)$
F	F	V	V	V	V	V
V	F	V	V	V	F	F
F	F	V	F	F	V	V
F	F	V	F	F	V	F
F	V	F	V	V	V	V
V	V	F	V	V	F	F
F	V	F	V	F	V	V
V	V	F	V	F	F	F

Las combinaciones que dan el valor V son VVF, FVF y FFF. Por lo tanto, una forma normal disyuntiva lógicamente equivalente es

$$((p_1 \wedge p_2 \wedge (\sim p_3)) \vee ((\sim p_1) \wedge p_2 \wedge (\sim p_3)) \vee ((\sim p_1) \wedge (\sim p_2) \wedge (\sim p_3)))$$

Así pues, la forma enunciativa dada es lógicamente equivalente a la negación de la anterior, la cual, por las leyes de De Morgan, es lógicamente equivalente a

$$(\sim(p_1 \wedge p_2 \wedge (\sim p_3)) \wedge (\sim((\sim p_1) \wedge p_2 \wedge (\sim p_3))) \wedge (\sim((\sim p_1) \wedge (\sim p_2) \wedge (\sim p_3))))$$

y a

$$(((\sim p_1 \vee (\sim p_2) \vee (\sim(\sim p_3))) \wedge ((\sim(\sim p_1) \vee (\sim p_2) \vee (\sim(\sim p_3))) \wedge ((\sim(\sim p_1) \vee (\sim(\sim p_2)) \vee (\sim(\sim p_3)))$$

y a

$$((\sim p_1) \vee (\sim p_2) \vee p_3) \wedge (p_1 \vee (\sim p_2) \vee p_3) \wedge (p_1 \vee p_2 \vee p_3)$$

que está en forma normal conjuntiva.

Ejercicios

12 Encuéntrense formas enunciativas en forma normal disyuntiva que sean lógicamente equivalentes a las siguientes:

(*a*) $(p \leftrightarrow q)$;
(*b*) $(p \rightarrow ((\sim q) \vee r))$;
(*c*) $((p \wedge q) \vee ((\sim q) \leftrightarrow r))$;
(*d*) $(\sim ((p \rightarrow (\sim q)) \rightarrow r)$;
(*e*) $(((p \rightarrow q) \rightarrow r) \rightarrow s)$.

13 Encuéntrense formas enunciativas en forma normal conjuntiva que sean lógicamente equivalentes a las siguientes:

(*a*) $(((\sim p) \vee q) \rightarrow r)$;
(*b*) $(p \leftrightarrow q)$;
(*c*) $(p \wedge q \wedge r) \vee ((\sim p) \wedge (\sim q) \wedge r)$;
(*d*) $(((p \rightarrow q) \rightarrow r) \rightarrow s)$.

1.5 Conjuntos adecuados de conectivas

Definición 1.23

Un conjunto *adecuado* de conectivas es un conjunto tal que toda función de verdad puede representarse por medio de una forma enunciativa que contenga solamente conectivas del conjunto.

▷ Una de las consecuencias de la discusión precedente es que $\{ \sim, \wedge, \vee \}$ es un conjunto adecuado de conectivas. Podemos utilizar este conjunto para encontrar otros.

Proposición 1.24

Los pares $\{ \sim, \wedge \}$, $\{ \sim, \vee \}$ y $\{ \sim, \rightarrow \}$ son conjuntos adecuados de conectivas.

Demostración: En primer lugar, cualesquiera que sean las formas enunciativas $\mathscr{A}$ y $\mathscr{B}$, $(\mathscr{A} \vee \mathscr{B})$ es lógicamente equivalente a $(\sim ((\sim \mathscr{A}) \wedge (\sim \mathscr{B})))$, de modo que toda forma enunciativa que contenga $\{ \sim, \wedge, \vee \}$ puede transformarse en una forma enunciativa que contenga solamente $\sim$ y $\wedge$.

En segundo lugar, podemos usar análogamente la equivalencia lógica entre $(\mathscr{A} \wedge \mathscr{B})$ y $(\sim ((\sim \mathscr{A}) \vee (\sim \mathscr{B})))$ para ver que $\{ \sim, \vee \}$ es adecuado.

En tercer lugar, hemos de encontrar formas enunciativas lógica-

mente equivalentes a $(\mathscr{A} \wedge \mathscr{B})$ y $(\mathscr{A} \vee \mathscr{B})$ en las que aparezcan solamente $\sim$ y $\rightarrow$.

$(\mathscr{A} \wedge \mathscr{B})$ es lógicamente equivalente a $(\sim(\mathscr{A} \rightarrow (\sim \mathscr{B})))$.
$(\mathscr{A} \vee \mathscr{B})$ es lógicamente equivalente a $((\sim \mathscr{A}) \rightarrow \mathscr{B})$.

Estas equivalencias pueden usarse para transformar cualquier forma enunciativa en la que figuren $\{\sim, \vee, \wedge\}$ en una forma enunciativa lógicamente equivalente en la que figuren solamente $\sim$ y $\rightarrow$.

Ejemplo 1.25

$(((\sim p_1) \vee p_2) \rightarrow p_3)$ es lógicamente equivalente a cada una de las formas enunciativas siguientes:

(*a*) $(\sim((\sim p_1) \vee p_2) \vee p_3)$
(*b*) $(\sim(\sim(p_1 \wedge (\sim p_2)) \wedge (\sim p_3)))$
(*c*) $((p_1 \rightarrow p_2) \rightarrow p_3)$

▷ A partir de nuestras cinco conectivas hay tres modos de escoger un par adecuado. Ningún otro par es adecuado. Para convencernos de esto, consideremos primeramente un par de conectivas distintas de $\sim$, y preguntémonos: ¿Puede expresarse una función de verdad que tome siempre el valor F mediante una forma enunciativa que use solamente ese par de conectivas? La respuesta es forzosamente negativa, ya que dando a todas las variables de enunciado de una tal forma enunciativa el valor V la forma enunciativa total tomaría necesariamente el valor V. No hay modo de que la forma o una parte suya tome el valor F bajo esta asignación de valores de verdad. Así pues, ninguna forma enunciativa en la que sólo figuren las conectivas $\wedge$, $\vee$, $\rightarrow$, $\leftrightarrow$ puede ser una contradicción. Por tanto, ningún subconjunto de este conjunto de conectivas puede ser adecuado. Se deja al lector la verificación de que $\{\sim, \leftrightarrow\}$ no es un conjunto adecuado.

Existen otras conectivas; de hecho, cualquier tabla de verdad podría emplearse para definir una conectiva, pero su significado intuitivo sería menos claro. No obstante, hay dos que merecen mencionarse.

Nor

Se denota por $\downarrow$, y su tabla de verdad es la siguiente:

p	q	$(p \downarrow q)$
V	V	F
V	F	F
F	V	F
F	F	V

Nand

Se denota $|$, y su tabla de verdad es la siguiente:

p	q	$(p \mid q)$
V	V	F
V	F	V
F	V	V
F	F	V

La razón del interés de estas conectivas (que tiene consecuencias en el diseño y estudio de computadoras) viene dada por la proposición siguiente:

Proposición 1.26

Los conjuntos unitarios $\{\downarrow\}$ y $\{|\}$ son conjuntos adecuados de conectivas, es decir, toda función de verdad puede expresarse mediante una forma enunciativa en la que sólo aparece $\downarrow$ (respectivamente $|$).

Demostración: Basta con que expresemos $\sim$ y $\wedge$, o bien $\sim$ y $\vee$, en términos de $\downarrow$ y en términos de $|$, ya que sabemos que $\{\sim, \wedge\}$ y $\{\sim, \vee\}$ son conjuntos adecuados. En primer lugar, observemos que

$(\sim p)$ es lógicamente a $(p \downarrow p)$,

y

$(p \wedge q)$ es lógicamente equivalente a $((p \downarrow p) \downarrow (q \downarrow q))$.

En segundo lugar,

$(\sim p)$ es lógicamente equivalente a $(p \mid p)$,

y

$(p \vee q)$ es lógicamente equivalente a $((p \mid p) \mid (q \mid q))$.

La verificación tiene lugar del modo usual, construyendo tablas de verdad, y se deja como ejercicio.

Ejemplo 1.27

Encuéntrese una forma enunciativa en la que sólo figure $\downarrow$ y que sea equivalente a $(p \rightarrow q)$.

$(p \rightarrow q)$ es lógicamente equivalente a $(\sim(p \wedge (\sim q))$

y con ello a

$(\sim(p \wedge (q \downarrow q))$

y con ello a

$$(\sim((p \downarrow p) \downarrow [(q \downarrow q) \downarrow (q \downarrow q)])$$

y con ello a

$$\{(p \downarrow p) \downarrow [(q \downarrow q) \downarrow (q \downarrow q)]\} \downarrow \{(p \downarrow p) \downarrow [(q \downarrow q) \downarrow (q \downarrow q)]\}$$

Este ejemplo ilustra el precio que hay que pagar en términos de complicación y longitud si se desea usar una única conectiva.

Ejercicios

14 Encuéntrense formas enunciativas en las que sólo figuren las conectivas $\sim$ y $\vee$, que sean lógicamente equivalentes a las siguientes:

(*a*) $(p \rightarrow (q \rightarrow r))$;
(*b*) $(((\sim p) \wedge (\sim q)) \rightarrow ((\sim r) \wedge s))$;
(*c*) $(p \leftrightarrow q)$.

15 Encuéntrense formas enunciativas en las que sólo figuren las conectivas $\sim$ y $\wedge$, que sean lógicamente equivalentes a las siguientes:

(*a*) $(p \rightarrow (q \rightarrow r))$;
(*b*) $((p \vee q \vee r) \wedge ((\sim p) \vee (\sim q) \vee (\sim r)))$;
(*c*) $((p \leftrightarrow (\sim q)) \leftrightarrow r)$.

16 Encuéntrense formas enunciativas en las que sólo figuren las conectivas $\sim$ y $\rightarrow$, que sean lógicamente equivalentes a las siguientes:

(*a*) $((p \wedge q) \vee (r \wedge s))$;
(*b*) $(p \leftrightarrow q)$;
(*c*) $(p \wedge q \wedge r)$.

17 (*a*) Demuéstrese que $\{\wedge, \vee\}$ no es un conjunto adecuado de conectivas.
(*b*) (Más difícil.) Demuéstrese que $\{\sim, \leftrightarrow\}$ no es un conjunto adecuado de conectivas.

18 Encuéntrese una forma enunciativa en la que sólo figure la conectiva $|$, que sea lógicamente equivalente a $(p \rightarrow q)$.

19 Demuéstrese que no existen conectivas binarias, aparte de $\downarrow$ y $|$, que constituyen por sí mismas un conjunto adecuado de conectivas. (Indicación: Considérese la tabla de verdad de cualquier conectiva así.)

1.6 Argumentaciones y validez

Volvamos a la consideración de argumentaciones. Por el momento hemos de restringirnos a argumentaciones cuyas premisas y conclusión sean enunciados, simples o compuestos, en el sentido definido al comienzo del capítulo. Vimos que lo importante era la «forma» de la argumentación, más bien que los significados de los enunciados que

intervienen. Consideraremos, pues, *formas argumentativas.* En un ejemplo previo nos encontramos con la forma argumentativa.

$$(p \rightarrow q)$$
$$p$$
$$\therefore\ q$$

En general, una forma argumentativa es una sucesión finita de formas enunciativas, de las cuales la última se considera como la conclusión y las restantes como las premisas.

Al tratar de decidir y definir qué es lo que constituye una forma argumentativa «válida», volvemos a tropezar con el mismo tipo de dificultad que ya tuvimos en relación con el símbolo de implicación. Al asignar valores de verdad a las variables de enunciado que aparecen en una forma argumentativa, podemos encontrarnos con que la conclusión es falsa y una o más de las premisas son, asimismo, falsas. ¿Justifican las premisas falsas una conclusión falsa? En cierto sentido, la pregunta es irrelevante, puesto que en el uso normal una argumentación se emplea solamente para demostrar que una cierta conclusión se deduce de premisas conocidas. Por lo tanto, todo lo que exigimos a una forma argumentativa válida es que, bajo cualquier asignación de valores de verdad a las variables de enunciado, si todas las premisas toman el valor *V*, la conclusión toma también el valor *V*. Equivalentemente, podemos hacer la siguiente definición:

Definición 1.28

La forma argumentativa

$$\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n;\ \therefore \mathscr{A}$$

es *inválida* si es posible asignar valores de verdad a las variables de enunciado que aparecen en ella, de tal manera que $\mathscr{A}_1, \ldots, \mathscr{A}_n$ tomen el valor *V* y $\mathscr{A}$ tome el valor *F*. En otro caso, la forma argumentativa es válida.

▷ Se nos presenta ahora el problema de comprobar si una forma argumentativa dada es o no válida. Consideremos el ejemplo sencillo: $(p \rightarrow q), p; \therefore q$. Construimos una tabla de verdad teniendo en cuenta todas las formas enunciativas que aparecen como premisas o conclusión.

p	q	$(p \rightarrow q)$
V	*V*	*V*
V	*F*	*F*
F	*V*	*V*
F	*F*	*V*

Las dos premisas toman simultáneamente el valor V tan sólo en la primera fila, y ocurre que la conclusión también toma el valor V en esta fila. Así pues, la forma argumentativa no es inválida, es decir, es válida.

Ejemplo 1.29

Investiguemos la validez de la forma argumentativa:

$$(p \rightarrow q),\ ((\sim q) \rightarrow r),\ r;\ \therefore p$$

Construimos la tabla de verdad:

$(p$	$\rightarrow$	$q)$	$((\sim$	$q)$	$\rightarrow$	$r)$	r	p	
V	V	V	F	V	V	V	V	V	$\leftarrow$
V	V	V	F	V	V	F	F	V	
V	F	F	V	F	V	V	V	V	
V	F	F	V	F	F	F	F	V	
F	V	V	F	V	V	V	V	F	$\leftarrow$
F	V	V	F	V	V	F	F	F	
F	V	F	V	F	V	V	V	F	$\leftarrow$
F	V	F	V	F	V	F	F	F	

Las tres filas marcadas con flechas son aquellas en las que todas las premisas toman el valor V. No obstante, en las filas quinta y séptima la conclusión toma el valor F. Así pues, la forma argumentativa es inválida.

Por consiguiente, disponemos de un método para decidir la validez de una forma argumentativa, que nos dará la respuesta en cada caso. No obstante, si el número de variables de enunciado es grande, la tabla de verdad será engorrosa y poco práctica. En cualquier caso, para nuestros propósitos no necesitamos la tabla de verdad completa. Nuestro método consiste en buscar una fila de un tipo particular, y esta búsqueda podemos llevarla a cabo de manera sistemática, en lugar de hacerla siguiendo el método de tanteo que supone construir la tabla completa. El procedimiento práctico se describe mejor en un ejemplo.

Ejemplo 1.30

Comprobemos la validez de la siguiente forma argumentativa.

$$((\sim p_1) \vee p_2),\ (p_1 \rightarrow (p_3 \wedge p_4)),\ (p_4 \rightarrow p_2);\ \therefore (p_2 \vee p_3).$$

Tratemos de asignar valores de verdad de manera que quede demostrada la invalidez de la forma argumentativa, es decir, de modo que las premisas se hagan verdaderas y la conclusión se haga falsa. Para que $(p_2 \vee p_3)$ tome el valor F, hemos de asignar F tanto a p_2

como a p_3. Seguidamente, para que $(p_4 \rightarrow p_2)$ tome el valor V, hemos de asignar F a p_4. Para que $((\sim p_1) \vee p_2)$ tome el valor V hemos de asignar F a p_1. Comprobando ahora el valor de verdad de la otra premisa $(p_1 \rightarrow (p_3 \wedge p_4))$ bajo estas asignaciones, vemos que resulta V. Así pues

p_1	p_2	p_3	p_4
F	F	F	F

es una asignación de valores de verdad bajo el cual todas las premisas toman el valor V y la conclusión toma el valor F. Por consiguiente, la forma argumentativa es inválida.

Nótese que si la forma argumentativa hubiese sido válida, hubiésemos sido incapaces de asignar valores de verdad de la manera inicialmente pretendida.

Ejemplo 1.31

Comprobemos la validez de la argumentación

$$(p_1 \rightarrow (p_2 \rightarrow p_3)),\ p_2 ;\ \therefore (p_1 \rightarrow p_3)$$

Tratemos de asignar valores de verdad a efectos de demostrar la invalidez de la forma argumentativa. Para que $(p_1 \rightarrow p_3)$ tome el valor F, p_1 tiene que tomar el valor V y p_3 el valor F. Hemos de exigir también que p_2 valga V. Bajo esta asignación de valores de verdad, la otra premisa, $(p_1 \rightarrow (p_2 \rightarrow p_3))$, toma el valor F. Así pues, es imposible asignar valores de verdad de modo que las premisas sean verdaderas y la conclusión falsa, y la argumentación es válida.

▷ La siguiente proposición explicita la conexión entre argumentaciones e implicaciones, ya mencionada brevemente más arriba.

Proposición 1.32

La forma argumentativa

$$\mathscr{A}_1, \ldots, \mathscr{A}_n ;\ \therefore \mathscr{A}$$

es válida si y sólo si la forma enunciativa

$$((\mathscr{A}_1 \wedge \ldots \wedge \mathscr{A}_n) \rightarrow \mathscr{A})$$

es una tautología.

Demostración: Supongamos primeramente que $\mathscr{A}_1, \ldots, \mathscr{A}_n ;\ \therefore \mathscr{A}$ es una forma argumentativa válida y que $((\mathscr{A}_1 \wedge \ldots \wedge \mathscr{A}_n) \rightarrow \mathscr{A})$ *no* es una tautología. Existe entonces una asignación de valores de verdad a las

variables de enunciado que intervengan, tal que $(\mathscr{A}_1 \wedge \ldots \wedge \mathscr{A}_n)$ toma el valor V y $\mathscr{A}$ toma el valor F. Bajo esta asignación, cada $\mathscr{A}_1$ toma el valor $V (1 \leqslant i \leqslant n)$ y $\mathscr{A}$ toma el valor F. Esto contradice la validez de la forma argumentativa, por lo cual $((\mathscr{A}_1 \wedge \ldots \wedge \mathscr{A}_n) \rightarrow \mathscr{A})$ tiene que ser una tautología.

Supongamos ahora, a la inversa, que $((\mathscr{A}_1 \wedge \ldots \wedge \mathscr{A}_n) \rightarrow \mathscr{A})$ es una tautología y que $\mathscr{A}_1, \ldots, \mathscr{A}_n; \therefore \mathscr{A}$ *no* es una forma argumentativa válida. Existe entonces una asignación de valores de verdad que hace tomar a cada $\mathscr{A}_i (1 \leqslant i \leqslant n)$ el valor V y a $\mathscr{A}$ el valor F, de modo que $((\mathscr{A}_1 \wedge \ldots \wedge \mathscr{A}_n) \rightarrow \mathscr{A})$ toma el valor F. Esto contradice la suposición de que esta forma enunciativa es una tautología, así que $\mathscr{A}_1, \ldots, \mathscr{A}_n; \therefore \mathscr{A}$ es una forma argumentativa válida.

Concluyamos el capítulo con una observación referente al familiar método matemático de «demostración por contradicción» o *reducción al absurdo*, que incidentalmente acaba de utilizarse en la demostración anterior.

Este tipo de demostración consiste en deducir una contradicción de la negación del enunciado que se quiere demostrar. El que este procedimiento es legítimo en el sentido de este capítulo, puede verse como sigue: Si tenemos una argumentación de la que se sabe que es un caso concreto de una forma argumentativa válida, y se sabe que su conclusión es falsa, entonces al menos una de las premisas debe ser falsa. Si se sabe que todas las premisas son verdaderas excepto una (la que se ha supuesto), puede deducirse legítimamente que ésta que se ha supuesto es la falsa.

Ejercicios

20 Para cada una de las siguientes argumentaciones, escríbase una forma argumentativa que se corresponda con ella y determínese si es válida o inválida.

(*a*) Si la función f no es continua, entonces la función g no es diferenciable. g es diferenciable. Así pues, f no es continua.

(*b*) Si Valdés ha instalado calefacción central, entonces ha vendido su coche o ha pedido dinero prestado al banco. Por tanto, si Valdés no ha vendido su coche, entonces no ha instalado calefacción central.

(*c*) Si hay petróleo en Poligonia, entonces o los expertos tienen razón o el gobierno está mintiendo. No hay petróleo en Poligonia, o si no los expertos se equivocan. Así pues, el gobierno no está mintiendo.

(*d*) Si U es un subespacio de V, entonces U es subconjunto de V, U contiene al vector cero y U es cerrado. U es un subconjunto de V, y si U es cerrado, entonces U contiene al vector cero. Así pues, si U es cerrado, entonces U es un subespacio de V.

21 Supóngase que $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n; \therefore \mathscr{A}$ es una forma argumentativa válida. Demuéstrese que $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_{n-1}; \therefore (\mathscr{A}_n \rightarrow \mathscr{A})$ es también una forma argumentativa válida.

22 Demuéstrese que lo siguiente es una forma argumentativa válida:

$p, (p|(q|r)); \therefore r$

2
Cálculo de enunciados formal

2.1 El sistema formal *L*

Nuestro estudio de la lógica está animado, al menos en parte, por el propósito de efectuar un análisis del proceso de deducción. En el primer capítulo hemos visto cómo abstraer la forma de los enunciados y las argumentaciones con el fin de ver más claramente las relaciones entre ellas y de dar una definición intuitiva de argumentación válida. No obstante, siguen en pie ciertas cuestiones. Por ejemplo, ¿podemos encontrar un procedimiento sencillo que nos permita construir una argumentación paso a paso, sabiendo que cada paso es válido? ¿En qué podríamos basar un procedimiento de este tipo? No podemos deducir a partir de la nada, sino que hemos de hacer algunas suposiciones iniciales. Para investigar este tipo de problemas, vamos a introducir la idea de *sistema deductivo formal.* Esto es en esencia la continuación de nuestro proceso de abstracción, a lo largo del cual llegamos a hacer abstracta la noción de demostración. La palabra «formal» aparece con frecuencia en libros de texto de lógica, sin que se dé explicación de ella. Se usa para referirse a una situación en la que se emplean símbolos cuyo comportamiento y propiedades están completamente determinados por un conjunto dado de reglas. En un sistema formal los símbolos carecen de significado, y al manejarlos hemos de tener cuidado de no presuponer nada de sus propiedades, salvo lo que se especifique en el sistema. Este es el único modo de estar seguros de que todas las suposiciones que hagamos a lo largo de una demostración son explícitas; y el hacer explícitas todas nuestras suposiciones es la única manera de que podamos descubrir algo fundamental acerca de la lógica.

En este libro nos ocuparemos de dos sistemas formales particulares, pero a veces necesitaremos tratar otros que son modificaciones de estos dos, de modo que vamos a comenzar dando una definición general de lo que constituye un sistema formal.

Para especificar un sistema formal se requieren:

1. Un alfabeto de símbolos.
2. Un conjunto de cadenas finitas de dichos símbolos, llamadas fórmulas bien formadas. Ha de imaginarse que éstas son las palabras y frases de nuestros lenguajes formales.
3. Un conjunto de fórmulas bien formadas, llamadas axiomas.
4. Un conjunto finito de «reglas de deducción», por ejemplo, reglas que permiten deducir una fórmula bien formada, tal como $\mathscr{A}$, como «consecuencia directa» de un conjunto finito de fórmulas bien formadas, tales como $\mathscr{A}_1, \ldots, \mathscr{A}_k$.

Dadas estas cuatro cosas, pueden construirse deducciones (que pueden o no estar relacionadas con la deducción lógica, en dependencia del sistema formal particular considerado) por medio de aplicaciones sucesivas de las reglas de deducción a partir de axiomas. Muy pronto precisaremos esto.

Notación: De aquí en adelante abreviaremos «fórmula bien formada» poniendo «*fbf*».

Definición 2.1

El *sistema formal L del cálculo de enunciados* se define como sigue:

1. Alfabeto de símbolos (infinito):

$$\sim,\ \rightarrow,\ (\ ,\ ),\ p_1,\ p_2,\ p_3,\ \ldots,$$

2. Conjunto de *fbfs*. En lugar de especificarlo explícitamente damos una regla inductiva con tres partes (véase Definición 1.2):

(i) p_i es una *fbf* para todo $i \geqslant 1$.
(ii) Si $\mathscr{A}$ y $\mathscr{B}$ son *fbfs*, entonces $(\sim\mathscr{A})$ y $(\mathscr{A}\rightarrow\mathscr{B})$ son *fbfs*.
(iii) El conjunto de todas las *fbfs* es el generado por (i) e (ii).

3. Axiomas. Hay infinitos axiomas, así que no podemos escribirlos todos. No obstante, podemos especificarlos por medio de tres *esquemas de axiomas*. Cualesquiera que sean las *fbfs* $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$, las *fbfs* siguientes son axiomas de *L:*

$(L1)$ $(\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{C}))$.

$(L2)$ $((\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{C}))\rightarrow((\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\mathscr{A}\rightarrow\mathscr{C})))$.

$(L3)$ $(((\sim\mathscr{A})\rightarrow(\sim\mathscr{B}))\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$.

Nótese que cada esquema de axioma tiene infinitas «realizaciones», según $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ varían sobre todas las *fbfs* de *L*.

4. Reglas de deducción. En *L* hay solamente una regla de deducción, la regla *modus ponens* (abreviadamente, *MP*), que afirma: De $\mathscr{A}$ y $(\mathscr{A}\rightarrow\mathscr{B})$ se deduce como consecuencia directa $\mathscr{B}$, siendo $\mathscr{A}$ y $\mathscr{B}$ *fbfs* cualesquiera de *L*.

▷ El alfabeto y el conjunto de *fbfs* se han escogido de modo que reflejen el desarrollo del capítulo anterior. Queremos que las *fbfs* representen de alguna manera las formas enunciativas, así que la definición sigue de cerca a la definición de forma enunciativa. Los símbolos $\wedge$, $\vee$, $\leftrightarrow$ no aparecen en el alfabeto de *L*, de modo que las expresiones en las que intervengan no son parte de *L*. No obstante, como ya hemos visto, $\{\sim, \rightarrow\}$ es un conjunto adecuado de conectivas, de manera que toda función de verdad estará representada por alguna *fbf* de *L*, y toda forma enunciativa será lógicamente equivalente a alguna *fbf* de *L*. (Téngase presente, sin embargo, que las nociones de forma enunciativa y equivalencia lógica pertenecen al capítulo 1 y no tienen lugar en el sistema formal *L*.) En *L* hemos limitado el número de conectivas a fin de hacer el sistema formal más sencillo y para poder escribir en poco espacio un conjunto de axiomas y reglas de deducción. Si hubiésemos incluido $\wedge$, por ejemplo, en el alfabeto de símbolos, tendríamos que haber incluido también axiomas y/o reglas de deducción para gobernar su comportamiento (y para hacer explícita su conexión con el símbolo $\rightarrow$), ya que los símbolos de nuestro lenguaje no tienen propiedades prefijadas; todas sus propiedades han de ser derivables a partir de la información contenida en la definición de *L*.

La regla de deducción de *L* parece razonable desde el punto de vista intuitivo. Esta regla corresponde a una de las maneras standard de proceder en una argumentación en lenguaje cotidiano. Los axiomas de *L* son la parte menos obvia del sistema. El lector hará bien en examinarlos de cerca, dándose cuenta de que si se consideran como formas enunciativas, son tautologías. Los axiomas han de estar presentes para proporcionar una base a partir de la cual deducir, y el conjunto que hemos escogido no es el único posible. Los esquemas de axiomas considerados más arriba resultan ser convenientes para las demostraciones de dos teoremas posteriores, el Teorema de Deducción y el Teorema de Adecuación. En el curso de la exposición se aclararán presumiblemente las razones que han aconsejado la elección de axiomas.

Debemos explicar ahora la naturaleza deductiva de *L*.

Definición 2.2

Una *demostración en L* es una sucesión finita de *fbfs*. $\mathscr{A}_1, \ldots, \mathscr{A}_n$ tal que para todo i $(1 \leqslant i \leqslant n)$, o $\mathscr{A}_i$ es un axioma de *L* o $\mathscr{A}_i$ se deduce de dos miembros anteriores de la sucesión, digamos $\mathscr{A}_j$ y $\mathscr{A}_k$ $(j<i,\ k<i)$ como consecuencia directa, aplicando la regla de deducción *MP*. Una tal demostración diremos que es una *demostración de* $\mathscr{A}_n$ *en L*, y también que $\mathscr{A}_n$ *es un teorema de L*.

Observaciones 2.3

(*a*) En la definición anterior, obsérvese que $\mathscr{A}_j$ y $\mathscr{A}_k$ deben ser necesariamente de las formas $\mathscr{B}$ y $(\mathscr{B}\rightarrow\mathscr{A}_i)$ o viceversa.

(*b*) Si $\mathscr{A}_1, \ldots, \mathscr{A}_n$ es una demostración en L y $k<n$, entonces $\mathscr{A}_1, \ldots, \mathscr{A}_k$ es también una demostración en L (evidentemente, satisface la definición), de modo que $\mathscr{A}_k$ es un teorema de L.

(*c*) Los axiomas de L son ciertamente teoremas de L. Sus demostraciones en L son sucesiones con un solo miembro.

Ejemplo 2.4

La siguiente sucesión finita es una demostración en L.

(1) $(p_1\rightarrow(p_2\rightarrow p_1))$ (caso particular de $(L1)$)
(2) $((p_1\rightarrow(p_2\rightarrow p_1))\rightarrow((p_1\rightarrow p_2)\rightarrow(p_1\rightarrow p_1)))$ $(L2)$
(3) $((p_1\rightarrow p_2)\rightarrow(p_1\rightarrow p_1))$ (de (1), (2) mediante MP)

Se deduce que $((p_1\rightarrow p_2)\rightarrow(p_1\rightarrow p_1))$ es un teorema de L.

Una demostración en L es una demostración a partir de los axiomas. Vamos a necesitar también el concepto más general de deducción a partir de un conjunto dado de *fbfs*.

Definición 2.5

Sea Γ un conjunto de *fbfs* de L (que pueden o no ser axiomas o teoremas de L). Una sucesión finita $\mathscr{A}_1, \ldots, \mathscr{A}_n$ de *fbfs* de L es una *deducción a partir de* Γ si para todo i $(1\leqslant i\leqslant n)$ se verifica alguna de las condiciones siguientes:

(*a*) $\mathscr{A}_i$ es un axioma de L,
(*b*) $\mathscr{A}_i$ es miembro de Γ,
(*c*) $\mathscr{A}_i$ se deduce directamente de dos miembros anteriores de la sucesión mediante MP.

Así pues, una dedución a partir de Γ es justamente una «demostración» en la cual los miembros de Γ se consideran temporalmente como axiomas.

El último miembro, $\mathscr{A}_n$, de una sucesión finita que sea una deducción a partir de Γ, se dice que es *deducible a partir de* Γ, o que es una consecuencia de Γ en L.

Si una *fbf* $\mathscr{A}$ es el último miembro de alguna deducción a partir de Γ, diremos que $\mathscr{A}$ es *derivable* a partir de Γ y escribiremos $\Gamma\mid\overline{}_L\mathscr{A}$.

Nótese que todo teorema de L es deducible a partir del conjunto vacío de *fbfs* (una demostración en L es una deducción a partir de ϕ), de manera que si $\mathscr{A}$ es un teorema de L podemos escribir $\phi\mid\overline{}_L\mathscr{A}$, o más sencillamente y para abreviar, $\mid\overline{}_L\mathscr{A}$.

Observación: Es importante recordar que «⊢» no es un símbolo de *L*, y que por lo tanto una expresión que lo contenga no puede ser parte de *L*. Por ejemplo, $\vdash_T \mathscr{A}$, lejos de ser parte de *L*, es un enunciado *acerca* de *L*, el enunciado que afirma que la *fbf* $\mathscr{A}$ es un teorema de *L*.

Ejemplo 2.6

Lo que sigue es una deducción de *L* que demuestra $\{\mathscr{A}, (\mathscr{B}\rightarrow(\mathscr{A}\rightarrow\mathscr{C}))\} \vdash_L (\mathscr{B}\rightarrow\mathscr{C})$ siendo $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ *fbf*s cualesquiera de *L*.

(1)	$\mathscr{A}$	hipótesis
(2)	$(\mathscr{B}\rightarrow(\mathscr{A}\rightarrow\mathscr{C}))$	hipótesis
(3)	$(\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$	(*L*1)
(4)	$(\mathscr{B}\rightarrow\mathscr{A})$	(1), (3) *MP*
(5)	$((\mathscr{B}\rightarrow(\mathscr{A}\rightarrow\mathscr{C}))\rightarrow((\mathscr{B}\rightarrow\mathscr{A})\rightarrow(\mathscr{B}\rightarrow\mathscr{C}))$	(*L*2)
(6)	$((\mathscr{B}\rightarrow\mathscr{A})\rightarrow(\mathscr{B}\rightarrow\mathscr{C}))$	(2), (5) *MP*
(7)	$(\mathscr{B}\rightarrow\mathscr{C})$	(4), (6) *MP*

▷ Este ejemplo y la observación que le precede sacan a la luz una distinción que importa recalcar: Del mismo modo que $\vdash_L \mathscr{A}$ es un enunciado acerca de *L*, el resultado del ejemplo es un resultado general sobre *L:*

Para *fbf*s $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ cualesquiera de *L*,

$$\{\mathscr{A}, (\mathscr{B}\rightarrow(\mathscr{A}\rightarrow\mathscr{C}))\}\vdash_L (\mathscr{B}\rightarrow\mathscr{C})$$

Este resultado acerca de *L* ciertamente no es parte de *L*. En nuestros procedimientos existen dos niveles, ya que estamos demostrando resultados acerca de demostraciones. Emplearemos la palabra «teorema» tan sólo para referirnos a *fbf*s del sistema formal que posean demostración en el sentido de la Definición 2.2. Para designar resultados, como el mencionado más arriba, acerca de sistemas formales, se usa a veces la palabra «metateorema». Los teoremas son ciertas *fbf*s, mientras que los metateoremas se escriben en lenguaje matemático ordinario. Nuestro uso de la palabra proposición tiene por objeto evitar confusiones. En general, nuestras proposiciones son metateoremas.

Nótese también que las letras cursivas $\mathscr{A}$, $\mathscr{B}$, etc., que hemos venido usando no son parte de *L*. Las usamos por conveniencia, para representar a *fbf*s de *L* no especificadas, o cuando hacemos aseveraciones generales sobre *L*.

Hemos construido el sistema formal *L* como un sistema en el cual ciertas *fbf*s pueden demostrarse como teoremas. Naturalmente, nos interesa saber qué *fbf*s de *L* son teoremas. Ahora bien, el único método de que disponemos para demostrar que una *fbf* es un teorema es exhi-

bir una sucesión finita de *fbfs* que constituya una demostración. Esto puede resultar un asunto engorroso y los métodos a emplear en cada caso particular no siempre son obvios.

Ejemplo 2.7

Para *fbfs* cualesquiera $\mathscr{A}$ y $\mathscr{B}$ de L

(*a*) $\vdash_L (\mathscr{A} \to \mathscr{A})$.

(*b*) $\vdash_L (\sim \mathscr{B} \to (\mathscr{B} \to \mathscr{A}))$.

Escribiremos para cada caso una demostración en L. Para (*a*):

(1)	$(\mathscr{A} \to ((\mathscr{A} \to \mathscr{A}) \to \mathscr{A})) \to ((\mathscr{A} \to (\mathscr{A} \to \mathscr{A})) \to (\mathscr{A} \to \mathscr{A}))$		$(L2)$
(2)	$(\mathscr{A} \to ((\mathscr{A} \to \mathscr{A}) \to \mathscr{A}))$		$(L1)$
(3)	$((\mathscr{A} \to (\mathscr{A} \to \mathscr{A})) \to (\mathscr{A} \to \mathscr{A}))$	(1), (2)	MP
(4)	$((\mathscr{A} \to (\mathscr{A} \to \mathscr{A}))$		$(L1)$
(5)	$(\mathscr{A} \to \mathscr{A})$	(3), (4)	MP

Para (*b*):

(1)	$(\sim \mathscr{B} \to (\sim \mathscr{A} \to \sim \mathscr{B}))$		$(L1)$
(2)	$((\sim \mathscr{A} \to \sim \mathscr{B}) \to (\mathscr{B} \to \mathscr{A}))$		$(L3)$
(3)	$((\sim \mathscr{A} \to \sim \mathscr{B}) \to (\mathscr{B} \to \mathscr{A})) \to (\sim \mathscr{B} \to ((\sim \mathscr{A} \to \sim \mathscr{B}) \to (\mathscr{B} \to \mathscr{A})))$		$(L1)$
(4)	$(\sim \mathscr{B} \to ((\sim \mathscr{A} \to \sim \mathscr{B}) \to (\mathscr{B} \to \mathscr{A})))$	(2), (3)	MP
(5)	$(\sim \mathscr{B} \to ((\sim \mathscr{A} \to \sim \mathscr{B}) \to (\mathscr{B} \to \mathscr{A}))) \to ((\sim \mathscr{B} \to (\sim \mathscr{A} \to \sim \mathscr{B})) \to (\sim \mathscr{B} \to (\mathscr{B} \to \mathscr{A})))$		$(L2)$
(6)	$(\sim \mathscr{B} \to (\sim \mathscr{A} \to \sim \mathscr{B})) \to (\sim \mathscr{B} \to (\mathscr{B} \to \mathscr{A}))$	(4), (5)	MP
(7)	$(\sim \mathscr{B} \to (\mathscr{B} \to \mathscr{A}))$	(1), (6)	MP

En lo anterior hemos sido menos estrictos que anteriormente en el uso de los paréntesis. Algunas de las expresiones empleadas en la demostración del caso (*b*) no son *fbfs*. Por ejemplo, (1) debería ser $((\sim \mathscr{B}) \to ((\sim \mathscr{A}) \to (\sim \mathscr{B})))$. No obstante, seguiremos abreviando *fbfs* de esta manera. Las ventajas que se obtienen así son obvias, pero hemos de tener cuidado de no omitir tantos paréntesis que la expresión resultante sea ambigua.

▷ Una manera de hacer menos ardua la demostración de teoremas es permitir en las demostraciones la inserción de *fbfs* para las que se ha obtenido previamente una demostración. Esto se corresponde con el procedimiento matemático standard de citar teoremas previamente demostrados. Otro modo consiste en hacer uso de ciertos metateoremas generales, algunos de los cuales tienen el efecto de reglas de inferencia adicionales. La principal herramienta es el resultado siguiente.

Proposición 2.8 (El Teorema de Deducción)

Si $\Gamma \cup \{\mathscr{A}\} \vdash_L \mathscr{B}$ entonces $\Gamma \vdash_L (\mathscr{A} \rightarrow \mathscr{B})$, siendo $\mathscr{A}$ y $\mathscr{B}$ *fbfs* de L y Γ un conjunto de *fbfs* de L (eventualmente vacío).

Demostración: La demostración es por inducción sobre el número de *fbfs* de la sucesión que constituye la deducción de $\mathscr{B}$ a partir de $\Gamma \cup \{\mathscr{A}\}$. Para el paso base, supongamos que esta sucesión tenga un solo miembro. Este miembro debe ser la propia $\mathscr{B}$, así que $\mathscr{B}$ es un axioma de L o $\mathscr{B}$ es miembro de $\Gamma \cup \{\mathscr{A}\}$.

Caso 1: $\mathscr{B}$ es un axioma de L. Lo que sigue es una deducción de $(\mathscr{A} \rightarrow \mathscr{B})$ a partir de Γ.

(1)	$\mathscr{B}$	axioma de L
(2)	$(\mathscr{B} \rightarrow (\mathscr{A} \rightarrow \mathscr{B}))$	$(L1)$
(3)	$(\mathscr{A} \rightarrow \mathscr{B})$	(1), (2) MP

Así pues, $\Gamma \vdash_L (\mathscr{A} \rightarrow \mathscr{B})$.

Caso 2: $\mathscr{B} \in \Gamma$. La siguiente deducción muestra que $\Gamma \vdash_L (\mathscr{A} \rightarrow \mathscr{B})$.

(1)	$\mathscr{B}$	miembro de Γ
(2)	$(\mathscr{B} \rightarrow (\mathscr{A} \rightarrow \mathscr{B}))$	$(L1)$
(3)	$(\mathscr{A} \rightarrow \mathscr{B})$	(1), (2) MP

Caso 3: $\mathscr{B}$ es $\mathscr{A}$. Hemos visto que $\vdash_L (\mathscr{A} \rightarrow \mathscr{A})$, de manera que la demostración de $(\mathscr{A} \rightarrow \mathscr{A})$ en L servirá como deducción de $(\mathscr{A} \rightarrow \mathscr{A})$ a partir de Γ. Por tanto, también en este caso tenemos $\Gamma \vdash_L (\mathscr{A} \rightarrow \mathscr{B})$. Esto completa el paso base.

Supongamos ahora que la deducción de $\mathscr{B}$ a partir de $\Gamma \cup \{\mathscr{A}\}$ es una sucesión de n miembros, siendo $n > 1$, y que la proposición se verifica para todas las *fbfs* $\mathscr{C}$ que pueden deducirse de $\Gamma \cup \{\mathscr{A}\}$ vía una sucesión de menos de n miembros. Ahora hay cuatro casos a considerar.

Caso 1: $\mathscr{B}$ es un axioma de L. Exactamente igual que en el Caso 1 de antes, demostramos que $\Gamma \vdash_L (\mathscr{A} \rightarrow \mathscr{B})$.

Caso 2: $\mathscr{B} \in \Gamma$. También en este caso, $\Gamma \vdash_L (\mathscr{A} \rightarrow \mathscr{B})$ como en el Caso 2 de antes.

Caso 3: $\mathscr{B}$ es $\mathscr{A}$. Como en el Caso 3 anterior.

Caso 4: $\mathscr{B}$ se obtiene de dos *fbfs* anteriores de la demostración mediante una aplicación de MP. Estas dos *fbfs* tendrán por fuerza las formas $\mathscr{C}$ y $(\mathscr{C} \rightarrow \mathscr{B})$, y cada una de ellas puede ciertamente deducirse de $\Gamma \cup \{\mathscr{A}\}$ mediante una sucesión de menos de n miembros. En cada caso, basta con omitir los miembros siguientes de la deducción original, y lo que queda es la sucesión deseada (cf. Observación 2.3(*b*)). Tenemos $\Gamma \cup \{\mathscr{A}\} \vdash_L \mathscr{C}$ y $\Gamma \cup \{\mathscr{A}\} \vdash_L (\mathscr{C} \rightarrow \mathscr{B})$, y, aplicando la hipótesis de inducción, $\Gamma \vdash_L (\mathscr{A} \rightarrow \mathscr{C})$ y $\Gamma \vdash_L (\mathscr{A} \rightarrow (\mathscr{C} \rightarrow \mathscr{B}))$.

La deducción requerida de $(\mathscr{A}\rightarrow\mathscr{B})$ a partir de Γ puede construirse ahora como sigue:

(1)		
⋮		deducción de $(\mathscr{A}\rightarrow\mathscr{C})$ a partir de Γ
(k)	$(\mathscr{A}\rightarrow\mathscr{C})$	
$(k+1)$		
⋮		deducción de $(\mathscr{A}\rightarrow(\mathscr{C}\rightarrow\mathscr{B}))$ a partir de Γ
(l)	$(\mathscr{A}\rightarrow(\mathscr{C}\rightarrow\mathscr{B}))$	
$(l+1)$	$(\mathscr{A}\rightarrow(\mathscr{C}\rightarrow\mathscr{B}))\rightarrow((\mathscr{A}\rightarrow\mathscr{C})\rightarrow(\mathscr{A}\rightarrow\mathscr{B}))$	$(L2)$
$(l+2)$	$(\mathscr{A}\rightarrow\mathscr{C})\rightarrow(\mathscr{A}\rightarrow\mathscr{B})$	(l), $(l+1)$ MP
$(l+3)$	$(\mathscr{A}\rightarrow\mathscr{B})$	(k), $(l+2)$ MP

$\therefore\quad \Gamma \vdash_L (\mathscr{A}\rightarrow\mathscr{B})$ en los cuatro casos.

Así pues, por el principio de inducción matemática, la proposición se verifica cualquiera que sea el número de *fbfs* de la deducción de $\mathscr{B}$ a partir de $\Gamma\cup\{\mathscr{A}\}$.

Nota. No hemos usado ningún caso particular de $(L3)$ en la demostración de esta proposición. Esto tiene importantes consecuencias en el estudio de otros sistemas formales que tienen otros conjuntos de axiomas diferentes.

▷ El recíproco del Teorema de Deducción es fácil de demostrar.

Proposición 2.9

Si $\Gamma \vdash_L (\mathscr{A}\rightarrow\mathscr{B})$ entonces $\Gamma\cup\{\mathscr{A}\}\vdash_L \mathscr{B}$, siendo $\mathscr{A}$ y $\mathscr{B}$ *fbfs* de L y Γ un conjunto (eventualmente vacío) de *fbfs* de L.

Demostración: Dada una deducción de $(\mathscr{A}\rightarrow\mathscr{B})$ a partir de Γ, deseamos construir una deducción de $\mathscr{B}$ a partir de $\Gamma\cup\{\mathscr{A}\}$.

(1)		
⋮		
(k)	$(\mathscr{A}\rightarrow\mathscr{B})$	deducción de $(\mathscr{A}\rightarrow\mathscr{B})$ a partir de Γ
$(k+1)$	$\mathscr{A}$	miembro de $\Gamma\cup\{\mathscr{A}\}$
$(k+2)$	$\mathscr{B}$	(k), $(k+1)$ MP

▷ El uso del Teorema de Deducción se ilustra en la demostración del resultado siguiente, que puede utilizarse como nueva regla de deducción.

Corolario 2.10

Dadas *fbfs* $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ cualesquiera de L,

$$\{(\mathscr{A}\to\mathscr{B}),\ (\mathscr{B}\to\mathscr{C})\}\vdash_L(\mathscr{A}\to\mathscr{C})$$

Demostración: Escribamos la deducción.

(1)	$(\mathscr{A}\to\mathscr{B})$	hipótesis
(2)	$(\mathscr{B}\to\mathscr{C})$	hipótesis
(3)	$\mathscr{A}$	hipótesis
(4)	$\mathscr{B}$	(1), (3) *MP*
(5)	$\mathscr{C}$	(2), (4) *MP*

Lo que hemos demostrado así es que

$$\{(\mathscr{A}\to\mathscr{B}),\ (\mathscr{B}\to\mathscr{C}),\mathscr{A}\}\vdash_L\mathscr{C} \qquad (*)$$

es decir,

$$\{(\mathscr{A}\to\mathscr{B}),\ (\mathscr{B}\to\mathscr{C})\}\cup\{\mathscr{A}\}\vdash_L\mathscr{C}$$

De este modo tenemos, por el Teorema de Deducción

$\{(\mathscr{A}\to\mathscr{B}),\ (\mathscr{B}\to\mathscr{C})\}\vdash_L(\mathscr{A}\to\mathscr{C})$ como se quería

▷ Este resultado se aplicará varias veces en lo que sigue; nos referiremos a él como regla del 'silogismo hipotético', y lo abreviaremos por *SH*.

Nota: Hay varias maneras de aplicar el Teorema de Deducción a (*) de más arriba. Puede deducirse también cualquiera de los resultados siguientes:

$$\{(\mathscr{A}\to\mathscr{B}),\ \mathscr{A}\}\vdash_L((\mathscr{B}\to\mathscr{C})\to\mathscr{C}),$$

$$\{(\mathscr{B}\to\mathscr{C}),\ \mathscr{A}\}\vdash_L((\mathscr{A}\to\mathscr{B})\to\mathscr{C}).$$

Aplicando de nuevo el Teorema de Deducción al resultado del corolario obtenemos

$$\{(\mathscr{A}\to\mathscr{B})\}\vdash_L((\mathscr{B}\to\mathscr{C})\to(\mathscr{A}\to\mathscr{C}))$$

y por tanto

$$\vdash_L((\mathscr{A}\to\mathscr{B})\to((\mathscr{B}\to\mathscr{C})\to(\mathscr{A}\to\mathscr{C}))).$$

Proposición 2.11

Dadas *fbfs* cualesquiera $\mathscr{A}$ y $\mathscr{B}$ de L, los dos siguientes son teoremas de L.

(*a*) $(\sim\mathscr{B}\to(\mathscr{B}\to\mathscr{A}))$

(*b*) $((\sim\mathscr{A}\to\mathscr{A})\to\mathscr{A})$.

Demostración: ((*a*) apareció en el ejemplo 2.7, pero lo incluimos aquí para ilustrar la simplificación resultante del uso de la nueva regla *SH*.)
Ad (*a*):

(1)	$(\sim\mathscr{B}\rightarrow(\sim\mathscr{A}\rightarrow\sim\mathscr{B}))$	(*L*1)
(2)	$(\sim\mathscr{A}\rightarrow\sim\mathscr{B})\rightarrow(\mathscr{B}\rightarrow\mathscr{A})$	(*L*3)
(3)	$(\sim\mathscr{B}\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$	(1), (2) *SH*

Ad (*b*):

(1)	$(\sim\mathscr{A}\rightarrow\mathscr{A})$	hipótesis
(2)	$(\sim\mathscr{A}\rightarrow(\sim\sim(\sim\mathscr{A}\rightarrow\mathscr{A})\rightarrow\sim\mathscr{A}))$	(*L*1)
(3)	$(\sim\sim(\sim\mathscr{A}\rightarrow\mathscr{A})\rightarrow\sim\mathscr{A})\rightarrow(\mathscr{A}\rightarrow\sim(\sim\mathscr{A}\rightarrow\mathscr{A}))$	(*L*3)
(4)	$(\sim\mathscr{A}\rightarrow(\mathscr{A}\rightarrow\sim(\sim\mathscr{A}\rightarrow\mathscr{A})))$	(2), (3) *SH*
(5)	$(\sim\mathscr{A}\rightarrow(\mathscr{A}\rightarrow\sim(\sim\mathscr{A}\rightarrow\mathscr{A})))\rightarrow((\sim\mathscr{A}\rightarrow\mathscr{A})\rightarrow(\sim\mathscr{A}\rightarrow\sim(\sim\mathscr{A}\rightarrow\mathscr{A})))$	(*L*2)
(6)	$(\sim\mathscr{A}\rightarrow\mathscr{A})\rightarrow(\sim\mathscr{A}\rightarrow\sim(\sim\mathscr{A}\rightarrow\mathscr{A}))$	(4),(5)*MP*
(7)	$(\sim\mathscr{A}\rightarrow\sim(\sim\mathscr{A}\rightarrow\mathscr{A}))$	(1),(6)*MP*
(8)	$(\sim\mathscr{A}\rightarrow\sim(\sim\mathscr{A}\rightarrow\mathscr{A}))\rightarrow((\sim\mathscr{A}\rightarrow\mathscr{A})\rightarrow\mathscr{A})$	(*L*3)
(9)	$(\sim\mathscr{A}\rightarrow\mathscr{A})\rightarrow\mathscr{A}$	(7),(8)*MP*
(10)	$\mathscr{A}$	(1),(9)*MP*

Así pues, $(\sim\mathscr{A}\rightarrow\mathscr{A})\vdash_L\mathscr{A}$,

$\therefore\vdash_L((\sim\mathscr{A}\rightarrow\mathscr{A})\rightarrow\mathscr{A})$, por el Teorema de Deducción. Estos resultados serán útiles más adelante.

Ejercicios

1 Escríbanse demostraciones en *L* para las siguientes *fbfs*.

(*a*) $(p_1\rightarrow p_2)\rightarrow((\sim p_1\rightarrow\sim p_2)\rightarrow(p_2\rightarrow p_1))$;
(*b*) $((p_1\rightarrow(p_2\rightarrow p_3))\rightarrow(p_1\rightarrow p_2))\rightarrow((p_1\rightarrow(p_2\rightarrow p_3))\rightarrow(p_1\rightarrow p_3))$;
(*c*) $(p_1\rightarrow(p_1\rightarrow p_2))\rightarrow(p_1\rightarrow p_2)$;
(*d*) $(p_1\rightarrow(p_2\rightarrow(p_1\rightarrow p_2)))$.

2 Demuéstrese que para *fbfs* cualesquiera $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ de *L* se verifica lo que sigue.

(*a*) $\{(\sim\mathscr{A})\}\vdash_L(\mathscr{A}\rightarrow\mathscr{B})$;
(*b*) $\{(\sim(\sim\mathscr{A}))\}\vdash_L\mathscr{A}$;
(*c*) $\{(\mathscr{A}\rightarrow\mathscr{B}),(\sim(\mathscr{B}\rightarrow\mathscr{C})\rightarrow(\sim\mathscr{A}))\}\vdash_L(\mathscr{A}\rightarrow\mathscr{C})$;
(*d*) $\{(\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{C}))\}\vdash_L(\mathscr{B}\rightarrow(\mathscr{A}\rightarrow\mathscr{C}))$.

3 Usando el Teorema de Deducción para *L*, demuéstrese que las siguientes *fbfs* son teoremas de *L*, siendo $\mathscr{A}$ y $\mathscr{B}$ *fbfs*, cualesquiera de *L*.

(*a*) $(\mathscr{A}\rightarrow(\sim(\sim\mathscr{A})))$;
(*b*) $((\mathscr{B}\rightarrow\mathscr{A})\rightarrow((\sim\mathscr{A})\rightarrow(\sim\mathscr{B})))$;
(*c*) $(((\mathscr{A}\rightarrow\mathscr{B})\rightarrow\mathscr{A})\rightarrow\mathscr{A})$;
(*d*) $(\sim(\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$.

4 Sea *L'* el sistema deductivo formal que difiere de *L* tan sólo en que tiene el

esquema de axiomas ($L3$) $((\sim\mathscr{A}\rightarrow\sim\mathscr{B})\rightarrow((\sim\mathscr{A}\rightarrow\mathscr{B})\rightarrow\mathscr{A})$. Demuéstrese que, dadas *fbfs*, cualesquiera $\mathscr{A}$ y $\mathscr{B}$ de L (y con ello de L'):

(i) $\vdash_{L'}((\sim\mathscr{A}\rightarrow\sim\mathscr{B})\rightarrow((\sim\mathscr{A}\rightarrow\mathscr{B})\rightarrow\mathscr{A}))$,

y

(ii) $\vdash_{L'}((\sim\mathscr{A}\rightarrow\sim\mathscr{B})\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$.

Dedúzcase que una *fbf* es un teorema de L si y sólo si es un teorema de L'.

5 La regla SH es un ejemplo de regla de deducción adicional legítima para L. ¿Es la siguiente regla legítima en el mismo sentido? A partir de las *fbfs* $\mathscr{B}$ y $(\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{C}))$, se deduce $(\mathscr{A}\rightarrow\mathscr{C})$.

2.2 El Teorema de Adecuación para L

No es una tarea muy remuneradora el demostrar que ciertas *fbfs* de L particulares son teoremas de L, como hemos hecho en la proposición 2.11. Como muestra la parte (*b*), a veces es difícil el saber cómo proceder, y el producto final puede ser muy complejo y distar mucho de ser una demostración intuitiva. No obstante, este aspecto de L no debe inquietarnos. La razón para definir L ha sido ante todo el intento de construir un sistema formal que refleje (por analogía) nuestras ideas intuitivas de deducción, validez y verdad, tratando de paso de aprender algo acerca de estas ideas.

El capítulo 1 nos ha proporcionado una noción de 'verdad lógica', el concepto de tautología. Parece razonable esperar que estas verdades lógicas se correspondan con los teoremas de L, y tratar de construir L según esta finalidad. El resto de este capítulo se dedica a demostrar que L posee esta propiedad. Este procedimiento nos proporcionará una cierta comprensión de la naturaleza y propiedades de los sistemas formales en general, que será útil en capítulos posteriores.

Pese a que los símbolos de L se consideran como puramente formales, L se ha definido de tal manera que pudimos interpretar las *fbfs* de L como formas enunciativas, estando representada cada función de verdad por alguna *fbf*. Así pues, aunque no podamos hablar de asignar valores de verdad a los símbolos de L de la misma manera que en el capítulo 1, podemos definir un procedimiento análogo.

Definición 2.12

Una *valoración* de L es una función v cuyo dominio es el conjunto de *fbfs* de L y cuyo rango es el conjunto $\{V, F\}$, tal que para *fbfs* cualesquiera $\mathscr{A}$, $\mathscr{B}$ de L,

(i) $v(\mathscr{A})\neq v(\sim\mathscr{A})$

y

(ii) $v(\mathscr{A}\rightarrow\mathscr{B})=F$ si y sólo si $v(\mathscr{A})=V$ y $v(\mathscr{B})=F$

Nótese que una 'asignación' arbitraria de 'valores de verdad' a los símbolos $p_1, p_2, \ldots$ de L conducirá a una valoración, ya que cada *fbfs* de L tomará (como forma enunciativa) exactamente uno de los dos valores de verdad bajo una tal asignación. (i) e (ii) se satisfarán trivialmente.

Definición 2.13

Una *fbf* de L es una *tautología* si para toda valoración v, $v(\mathscr{A}) = V$. Esto equivale a considerar $\mathscr{A}$ como forma enunciativa y aplicar la definición ya conocida.

▷ Demostraremos que una *fbf* de L es un teorema de L si y sólo si es una tautología. Ya estamos en condiciones de demostrar la implicación en un sentido.

Proposición 2.14 (El Teorema de Corrección)

Todo teorema de L es una tautología.

Demostración: Sea $\mathscr{A}$ un teorema de L. La demostración es por inducción sobre el número de *fbfs* de L miembros de una sucesión finita que constituya una demostración de $\mathscr{A}$ en L.

Para el paso base, supongamos que la demostración de $\mathscr{A}$ consta de una sola *fbf*, la propia $\mathscr{A}$. Entonces $\mathscr{A}$ tiene que ser un axioma de L. Todos los axiomas de L son tautologías. Esto se comprueba construyendo tablas de verdad, y se deja como ejercicio al lector.

Supongamos ahora que la demostración de $\mathscr{A}$ contiene n *fbfs*, siendo $n > 1$, y supongamos como hipótesis de inducción que todos los teoremas de L que poseen demostraciones de menos de n pasos son tautologías. O bien $\mathscr{A}$ es un axioma, en cuyo caso $\mathscr{A}$ es una tautología, o $\mathscr{A}$ se deduce mediante MP de dos *fbfs* anteriores en la demostración. Estas dos *fbfs* deberán tener las formas $\mathscr{B}$ y $(\mathscr{B} \rightarrow \mathscr{A})$. Pero $\mathscr{B}$ y $(\mathscr{B} \rightarrow \mathscr{A})$ son teoremas de L cuyas demostraciones son sucesiones de menos de n *fbfs* (la demostración de $\mathscr{A}$ truncada apropiadamente). Así pues, $\mathscr{B}$ y $(\mathscr{B} \rightarrow \mathscr{A})$ son tautologías por hipótesis de inducción, y de este modo, por la Proposición 1.9, $\mathscr{A}$ es una tautología.

Así pues, por el principio de inducción matemática, todo teorema de L es una tautología.

▷ Para demostrar el resultado recíproco, necesitamos dos nuevas ideas: *extensiones* de L y *consistencia*.

L tiene tres esquemas de axiomas, que son los puntos de partida para las demostraciones de teoremas. ¿Qué ocurriría si añadiésemos otro esquema de axiomas, o simplemente otro axioma? Tendríamos

más premisas de las que partir, de modo que, en general, podríamos esperar que fuese posible demostrar más teoremas. Todas las *fbfs* que fuesen teoremas previamente seguirían siéndolo, pero quizás algunas *fbfs* que no eran teoremas antes se convertirían en teoremas. De hecho, aparecerán nuevos teoremas si y sólo si el nuevo conjunto de axiomas contiene al menos una *fbf* que no fuese previamente un teorema. (El lector podrá encontrar fácilmente una demostración de ésto.)

Definición 2.15

Una *extensión* de L es un sistema formal obtenido alterando o ampliando el conjunto de axiomas de manera que todos los teoremas de L sigan siendo teoremas (habiéndose introducido eventualmente teoremas nuevos).

No hace falta más que consultar alguno de los muchos textos de lógica para comprobar que es posible reemplazar nuestros esquemas de axiomas ($L1$), ($L2$) y ($L3$) por otros, de tal manera que la clase de los teoremas no varíe. Por ejemplo, (véase el Ejercicio 2.4), ($L3$) puede reemplazarse por el esquema:

$$((\sim\mathscr{A}\rightarrow\sim\mathscr{B})\rightarrow((\sim\mathscr{A}\rightarrow\mathscr{B})\rightarrow\mathscr{A}))$$

sin alterar la clase de los teoremas.

Nota: Es posible que un sistema formal sea extensión de L sin tener axiomas en común con L

$\triangleright$ Si extendiésemos L a sistemas con mayor número de teoremas cada vez, lo más probable es que llegase a existir una *fbf* $\mathscr{A}$ tal que tanto $\mathscr{A}$ como $(\sim\mathscr{A})$ fuesen teoremas. Es evidente que una situación así no es deseable.

Definición 2.16

Una extensión de L es *consistente* si no existe ninguna *fbf* $\mathscr{A}$ de L tal que tanto $\mathscr{A}$ como $(\sim\mathscr{A})$ sean teoremas de la extensión.

Naturalmente, esta definición sería irrelevante si el propio L no fuese consistente.

Proposición 2.17

L es consistente.

Demostración: Supongamos que L no fuese consistente, por ejemplo que existiese una *fbf* $\mathscr{A}$ tal que $\vdash_L\mathscr{A}$ y $\vdash_L(\sim\mathscr{A})$. Entonces, por la proposi-

ción 2.14 (Teorema de Corrección), tanto $\mathscr{A}$ como $(\sim\mathscr{A})$ serían tautologías. Esto es imposible, ya que si $(\sim\mathscr{A})$ es una tautología, entonces $\mathscr{A}$ es una contradicción. Por lo tanto, L es consistente.

Proposición 2.18

Una extensión L^* de L es consistente si y sólo si existe una *fbf* que no es teorema de L^*.

Demostración: Sea L^* consistente. Entonces para toda *fbf* $\mathscr{A}$, o bien $\mathscr{A}$ o bien $(\sim\mathscr{A})$ no es teorema (ambas no pueden ser teoremas).

Recíprocamente, supongamos que L^* no es consistente. Demostremos que no hay *fbfs* que no sean teoremas de L^*, es decir, que toda *fbf* es teorema de L^*. Sea $\mathscr{A}$ cualquier *fbf*; L^* no es consistente, así que $\vdash_{L^*} \mathscr{B}$ y $\vdash_{L^*} (\sim\mathscr{B})$ para ciertas *fbfs* $\mathscr{B}$. Ahora bien, $\vdash_{L^*} (\sim\mathscr{B}\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$, por Proposición 2.11. Así, $\vdash_{L^*} (\sim\mathscr{B}\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$ pues L^* es extensión de L Aplicando dos veces MP, obtenemos ahora $\vdash_{L^*} \mathscr{A}$. Así pues, toda *fbf* es teorema de L^*, como se quería.

Han de recalcarse dos aspectos de esta proposición. A saber:

(*a*) En una extensión inconsistente de L, toda *fbf* es un teorema. Siempre que hagamos uso de extensiones de L debemos tener cuidado con la consistencia, ya que el valor de un sistema en el que todas las *fbfs* son teoremas es tan insignificante como el de un sistema en el que ninguna *fbf* es teorema.

(*b*) La condición suficiente de consistencia dada por la proposición es sorprendentemente débil: Que exista una sola *fbf* que no sea teorema. Esto es sorprendente, porque en cualquier sistema consistente habrá ciertamente muchas *fbfs* que no son teoremas: Por ejemplo, las negaciones de todos los teoremas son no-teoremas.

Pasemos ahora a una proposición que parece insignificante y puramente técnica, pero que usaremos vez tras vez en las demostraciones de resultados posteriores. Describe una circunstancia en la que puede obtenerse una extensión consistente.

Proposición 2.19

Sea L^* una extensión de L y sea $\mathscr{A}$ una *fbf* de L que no sea teorema de L^*. Entonces L^{**} es también consistente, siendo L^{**} la extensión de L obtenida añadiendo $(\sim\mathscr{A})$ como nuevo axioma a L^*.

Demostración: Sea $\mathscr{A}$ una *fbf* de L que no es teorema de L^*. Supongamos que L^{**} es inconsistente. Entonces, para alguna *fbf* $\mathscr{B}$, $\vdash_{L^{**}} \mathscr{B}$ y $\vdash_{L^{**}} (\sim\mathscr{B})$. Ahora bien, del mismo modo que en la demostración de la Pro-

posición 2.18, se deduce que $\vdash_{L^{**}} \mathscr{A}$. Pero L^{**} tan sólo se diferencia de L^{*} en que tiene a $(\sim\mathscr{A})$ como axioma adicional, así que $\vdash_{L^{**}} \mathscr{A}$ es equivalente a $(\sim\mathscr{A})\vdash_{L^{*}} \mathscr{A}$. (Una demostración en L^{**} es justamente una deducción a partir de $(\sim\mathscr{A})$ en L^{*}). Así pues, $\vdash_{L^{*}}((\sim\mathscr{A})\rightarrow\mathscr{A})$, por el Teorema de Deducción. Pero $\vdash_{L^{*}}(((\sim\mathscr{A})\rightarrow\mathscr{A})\rightarrow\mathscr{A})$, por la proposición 2.11, de modo que $\vdash_{L^{*}}(((\sim\mathscr{A})\rightarrow\mathscr{A})\rightarrow\mathscr{A})$.
Con MP obtenemos ahora

$$\vdash_{L^{*}} \mathscr{A}$$

Pero esto contradice la hipótesis de que $\mathscr{A}$ no es teorema de L^{*}. Así pues, L^{*} tiene que ser consistente.

▷ Obviamente, existe en alguna parte un límite a las *fbfs* que pueden incluirse como axiomas adicionales en una extensión de L, manteniendo la consistencia. La siguiente proposición tiene por objeto alcanzar este límite, pero describamos primero la situación en una definición.

Definición 2.20

Una extensión de L es *completa* si para toda *fbf* $\mathscr{A}$ o $\mathscr{A}$ o $(\sim\mathscr{A})$ es teorema de la extensión.

Observaciones: (*a*) L dista mucho de ser completa. Por ejemplo, p_1 es una *fbf* de L, y ni p_1 ni $(\sim p_1)$ son teoremas de L.

(*b*) Toda extensión inconsistente de L es obviamente completa, por la Proposición 2.18.

(*c*) Si L^{c} es una extensión consistente y completa de L, entonces cualquier otra extensión de L en la cual la clase de los teorema extienda a la clase de los teoremas de L^{c} es inconsistente. En efecto, supongamos que $\mathscr{A}$ no es teorema de L^{c}. Entonces $(\sim\mathscr{A})$ es teorema de L^{c}. Así pues, si $\mathscr{A}$ es un teorema de otra extensión, también lo es $(\sim\mathscr{A})$, de modo que esta otra extensión no puede ser consistente.

Proposición 2.21

Sea L^{*} una extensión consistente de L. Entonces existe una extensión consistente y completa de L^{*}.

(Nótese que aquí hemos generalizado nuestra terminología. Una extensión de L^{*} se obtiene alterando o ampliando el conjunto de axiomas de L^{*} de manera que el conjunto de teoremas aumente. Véase la Definición 2.15.)

Demostración: Sea $\mathscr{A}_0, \mathscr{A}_1, \mathscr{A}_2, \ldots$ una enumeración de todas las *fbfs* de L. Esta puede haberse construido de varias maneras —se aconseja

al lector que intente encontrar un método para producir una lista de este tipo. (Al hacerlo, será útil el estar familiarizado con construcciones referentes a conjuntos infinitos numerables).[1] Construyamos una sucesión $J_0, J_1, J_2, \ldots$ de extensiones de L^* como sigue.
Sea

$$J_0 = L^*$$

Si

$$\vdash_{J_0} \mathscr{A}_0, \text{ sea } J_1 = J_0$$

Si no $\vdash_{J_0} \mathscr{A}_0$, añádase $(\sim \mathscr{A}_0)$ como nuevo axioma para obtener J_1 a partir de J_0.

En general, dado $n \geqslant 1$, y para construir J_n a partir de J_{n-1}: Si $\vdash_{J_{n-1}} \mathscr{A}_{n-1}$, entonces $J_n = J_{n-1}$, y si no $\vdash_{J_{n-1}} \mathscr{A}_{n-1}$, sea J_n la extensión de J_{n-1} obtenida añadiendo $(\sim \mathscr{A}_{n-1})$ como nuevo axioma.

L^* es consistente, es decir, J_0 es consistente, por hipótesis. Dado $n \geqslant 1$, si J_{n-1} es consistente, entonces J_n es consistente, por la Proposición 2.19. Así pues, por inducción, todo $J_n (n \geqslant 0)$ es consistente. Definamos ahora J como aquella extensión de L^* que tiene como axiomas a aquellas *fbfs* que son axiomas de al menos uno de los J_n.

Demostraremos que J es consistente. Supongamos lo contrario. Entonces existe una *fbf.* $\mathscr{A}$ tal que $\vdash_J \mathscr{A}$ y $\vdash_J (\sim \mathscr{A})$. Ahora bien, las demostraciones de $\mathscr{A}$ y $(\sim \mathscr{A})$ en J son sucesiones finitas de *fbfs*, de modo que cada demostración solamente puede contener casos particulares de un número finito de axiomas de J. Así pues, debe existir un n suficientemente grande como para que todos estos axiomas utilizados sean axiomas de J_n. Se deduce que $\vdash_{J_n} \mathscr{A}$ y $\vdash_{J_n} (\sim \mathscr{A})$. Esto contradice la consistencia de J_n, con lo que J debe ser consistente.

Queda por demostrar que J es completo. Sea $\mathscr{A}$ una *fbf.* de L. $\mathscr{A}$ debe aparecer en la lista $\mathscr{A}_0, \mathscr{A}_1, \mathscr{A}_2, \ldots$, digamos que $\mathscr{A}$ es $\mathscr{A}_k$. Si $\vdash_{J_k} \mathscr{A}_k$, entonces $\vdash_J \mathscr{A}_k$, puesto que J es una extensión de J_k. Si no $\vdash_{J_k} \mathscr{A}_k$, entonces de acuerdo con la construcción de J_{k+1}, $(\sim \mathscr{A}_k)$ es un axioma de J_{k+1}, con lo que $\vdash_{J_{k+1}} (\sim \mathscr{A}_k)$. Esto implica que $\vdash_J (\sim \mathscr{A}_k)$. Así, en todo caso tenemos $\vdash_J \mathscr{A}$ o $\vdash_J (\sim \mathscr{A})$, con lo que J es completo.

Proposición 2.22

Si L^* es una extensión consistente de L, entonces existe una valoración en la cual todo teorema de L^* toma el valor V.

[1] Véase el Apéndice.

Demostración: Definamos v sobre *fbfs* de L poniendo:

$$v(\mathscr{A}) = V \text{ si } \vdash_J \mathscr{A},$$

y

$$v(\mathscr{A}) = F \text{ si } \vdash_J (\sim \mathscr{A}),$$

siendo J una extensión consistente y completa de L^*, como la dada en la demostración de la Proposición 2.21. Nótese que v está definida sobre todas las *fbfs*, por ser J completa. Ahora bien, $v(\mathscr{A}) \neq v(\sim \mathscr{A})$ para toda *fbf*. $\mathscr{A}$, ya que J es consistente, y queda por demostrar que $v(\mathscr{A} \to \mathscr{B}) = F$ si y sólo si $v(\mathscr{A}) = V$ y $v(\mathscr{B}) = F$. Supongamos primero que $v(\mathscr{A}) = V$, $v(\mathscr{B}) = F$ y $v(\mathscr{A} \to \mathscr{B}) = V$. Entonces $\vdash_J \mathscr{A}$, $\vdash_J (\sim \mathscr{B})$ y $\vdash_J (\mathscr{A} \to \mathscr{B})$. Se deduce que $\vdash_J \mathscr{B}$, por *MP*, en contradicción con la consistencia de J. Recíprocamente, supongamos que $v(\mathscr{A} \to \mathscr{B}) = F$ y o bien $\vdash_J (\sim \mathscr{A})$ o bien $\vdash_J \mathscr{B}$. Ahora bien

$$\vdash_J (\sim \mathscr{A} \to (\sim \mathscr{B} \to \sim \mathscr{A}))$$

y

$$\vdash_J (\mathscr{B} \to (\mathscr{A} \to \mathscr{B}))$$

de modo que, por *MP*

$$\vdash_J (\sim \mathscr{B} \to \sim \mathscr{A}) \text{ o } \vdash_J (\mathscr{A} \to \mathscr{B}).$$

Pero $\vdash_J ((\sim \mathscr{B} \to \sim \mathscr{A}) \to (\mathscr{A} \to \mathscr{B}))$, luego en cualquiera de los dos casos tenemos $\vdash_J (\mathscr{A} \to \mathscr{B})$, en contradicción con la consistencia de J. Así pues, $v(\mathscr{A} \to \mathscr{B}) = F$ implica $v(\mathscr{A}) = V$ y $v(\mathscr{B}) = F$, con lo que v es una valoración.

Sea ahora $\mathscr{A}$ un teorema de L^*. Entonces $\vdash_J \mathscr{A}$, pues J es una extensión de L^*. Con ello, $v(\mathscr{A}) = V$.

▷ Ahora estamos en condiciones de demostrar el resultado que deseábamos.

Proposición 2.23 (El Teorema de Adecuación para L)

Si $\mathscr{A}$ es una *fbf* de L y $\mathscr{A}$ es una tautología, entonces $\vdash_L \mathscr{A}$.

Demostración: Sea $\mathscr{A}$ una *fbf* de L que es tautología, y supongamos que $\mathscr{A}$ no es un teorema de L. Entonces la extensión L^*, obtenida añadiendo $(\sim \mathscr{A})$ como nuevo axioma, es consistente, por la Proposición 2.19. Así pues, existe una valoración v que da a todo teorema de L^* el valor V. En particular, $v(\sim \mathscr{A}) = V$. Pero $v(\sim \mathscr{A}) = V$, ya que $\mathscr{A}$ es una tautología, y llegamos a una contradición. Luego $\mathscr{A}$ es un teorema de L.

▷ Ahora ya hemos comprobado que el sistema formal *L* tiene la principal propiedad que debería tener: Que las *fbfs* derivables en él sean precisamente las 'lógicamente verdaderas'. Los axiomas y la regla de deducción de *L* caracterizan la deducción lógica, al menos en este contexto. El valor de nuestro estudio de *L* radica en esto y no en el estudio detallado de *fbfs*, demostraciones y teoremas de *L*.

Las ideas y métodos que hemos utilizado para demostrar el Teorema de Adecuación son bastantes fuertes y tendrán más adelante otras aplicaciones, pese a que su uso aquí ha sido el de meras herramientas para un propósito particular. En la literatura hay muchas otras demostraciones del Teorema de Adecuación, y algunas de ellas utilizan métodos totalmente diferentes. Hemos usado este método debido a que más tarde podremos aplicar más o menos el mismo procedimiento para demostrar un Teorema de Adecuación análogo para el sistema formal más complicado del cálculo de predicados. De hecho, toda nuestra discusión del sistema *L* ha tenido por objeto introducir las ideas de la materia más bien que estudiar el cálculo de enunciados por sí mismo. En lo que se refiere al cálculo de enunciados, el Capítulo 1 nos proporciona ya una visión suficiente. Las tablas de verdad nos dan toda la información necesaria acerca de formas enunciativas y formas argumentativas particulares, y utilizándolas podemos distinguir de manera efectiva entre tautologías, contradicciones y otras formas enunciativas. La consecuencia que esto trae consigo para *L* es importante y útil, así que la incluimos como proposición.

Proposición 2.24

L es *decidible*, es decir, existe un método efectivo para decidir si una *fbf* dada de *L* es o no un teorema de *L*.

Demostración: Para decidir si una *fbf* $\mathscr{A}$ es o no teorema de *L*, basta considerarla como forma enunciativa y construir su tabla de verdad. Es un teorema si y sólo si es una tautología.

Observación 2.25

Esto hace innecesario el seguir construyendo demostraciones en *L*. Las tablas de verdad proporcionan un método mecánico, aunque no siempre rápido, para demostrar si una *fbf.* dada es teorema de *L*. Pero, naturalmente, esto no lo sabíamos hasta ahora, de modo que la demostración de la Proposición 2.11, por ejemplo, no puede cambiarse, pues su resultado se necesitaba en la demostración del Teorema de Adecuación.

Ejercicios

6 Demuéstrese que todo axioma de L es una tautología.

7 Sea $\mathscr{A}$ una *fbf* de L y sea L^+ la extensión de L obtenida añadiendo $\mathscr{A}$ como nuevo axioma. Demuéstrese que el conjunto de los teoremas de L^+ es diferente del conjunto de los teoremas de L si y sólo si $\mathscr{A}$ no es teorema de L

8 Sea $\mathscr{A}$ la *fbf* $((\sim p_1 \rightarrow p_2) \rightarrow (p_1 \rightarrow \sim p_2))$. Demuéstrese que L^+, obtenido añadiendo esta $\mathscr{A}$ como nuevo axioma, tiene un conjunto de teoremas mayor que el de L. ¿Es L^+ una extensión consistente de L?

9 Demuéstrese que si $\mathscr{B}$ es una contradicción, entonces $\mathscr{B}$ no puede ser teorema de ninguna extensión consistente de L.

10 Sea L^{++} la extensión de L obtenida añadiendo como cuarto *esquema* de axiomas:

$$((\sim \mathscr{A} \rightarrow \mathscr{B}) \rightarrow (\mathscr{A} \rightarrow \sim \mathscr{B}))$$

Demuéstrese que L^{++} es inconsistente. (Sugerencia: Véase el Ejercicio 7 del Capítulo 1).

11 Sea J una extensión consistente y completa de L, y sea $\mathscr{A}$ una *fbf* de L. Demuéstrese que la extensión de J obtenida añadiendo $\mathscr{A}$ como nuevo axioma es consistente si y sólo si $\mathscr{A}$ es un teorema de J.

12 Sea $\mathscr{A}$ una *fbf* de L en la que intervengan las letras de enunciado $p_1, \ldots, p_n$, y sean $\mathscr{A}_1, \mathscr{A}_2, \ldots, \mathscr{A}_n$ *fbfs* cualesquiera de L. Sea $\mathscr{B}$ la *fbf* de L obtenida sustituyendo cada intervención de p_i en $\mathscr{A}$ por $\mathscr{A}_i (1 \leqslant i \leqslant n)$. Demuéstrese que si $\mathscr{A}$ es un teorema de L, entonces $\mathscr{B}$ es un teorema de L.

3
Cálculo de predicados informal

3.1 Predicados y cuantificadores

En el Capítulo 1 hemos analizado frases y argumentaciones, descomponiéndolas en enunciados constituyentes simples, y considerando éstos como las piezas de la construcción. De este modo hemos podido descubrir algo de lo que hace válida a una argumentación. No obstante, existen argumentaciones que no son susceptibles de un tratamiento de este tipo. Por ejemplo, escribamos uno de los ejemplos del Capítulo 1 de manera ligeramente distinta:

Todos los hombres son mortales
Sócrates es un hombre
$\therefore$ Sócrates es mortal.

Intuitivamente, consideraríamos esto como ejemplo de argumentación válida, pero si tratamos de simbolizar su forma como hicimos en el Capítulo 1, lo que obtenemos es $p, q, \therefore r$. Según el Capítulo 1, ésta no es una forma argumentativa válida.

La validez en este caso no depende de las relaciones entre las premisas y la conclusión en tanto que enunciados simples, sino de relaciones entre *partes* de los enunciados que intervienen y entre las formas de éstos. Si quisiésemos aclarar más esto encontrando la «forma argumentativa» correspondiente, nos encontraríamos con algo como:

Todos los As son B
C es un A
$\therefore$ C es B

Aquí hay dos puntos a tratar: Primero la naturaleza general de la premisa «Todos los As son B»; y segundo, el uso de símbolos para representar partes de enunciados simples. Estos puntos corresponden, respectivamente, a las ideas de «cuantificador» y «predicado». Todo enunciado simple en castellano tiene un sujeto y un predicado, cada

uno de los cuales puede consistir en una sola palabra, una frase breve o toda una cláusula. Hablando muy groseramente, el sujeto es la cosa acerca de la cual el enunciado está afirmando algo, y el predicado se refiere a una «propiedad» que posee el sujeto.

Ejemplo 3.1

En cada uno de los siguientes enunciados, se ha subrayado el sujeto y el resto es el predicado.

(*a*) Sócrates es un hombre.
(*b*) Yo escribo libros.
(*c*) El número cuya raíz es -1 no es real.
(*d*) El mundo nos debe a todos el sustento.

Resulta conveniente representar los predicados mediante letras mayúsculas A, B, C, ..., y los sujetos mediante letras minúsculas, con lo cual enunciados tales como los de más arriba se simbolizan del modo siguiente:

(*a*) $H(s)$ simboliza «Sócrates es un hombre», siendo H una letra de predicado que simboliza «es un hombre», y s simboliza a Sócrates. Podríamos análogamente simbolizar «Napoleón es un hombre» poniendo $H(n)$, donde n simboliza a Napoleón.

(*b*) $L(i)$ puede simbolizar «Yo escribo libros» de manera parecida.

(*c*) En este caso nuestro predicado es una negación, de modo que podemos elegir. Podemos escoger R que signifique «no es real», con lo que el enunciado tomará la forma $R(j)$, donde j representa al número cuya raíz es -1. O podemos escoger S que signifique «es real», con lo que el enunciado será $(\sim S(j))$.

(*d*) $V(m)$, análogamente a (*a*) y (*b*).

Queda claro que los enunciados compuestos también pueden simbolizarse de esta manera, simbolizando todos los enunciados simples que los constituyen.

▷¿Qué ocurre ahora con enunciados tales como «todos los hombres son mortales»? Necesitamos algo más que un análisis de sujeto y predicado, ya que el significado del enunciado depende de la fuerza de la palabra «todos». Consideremos otro ejemplo:

Todo entero tiene un factor primo.

En el simbolismo matemático ordinario, escribiríamos esto así:

Para todo x, si x es un entero entonces x tiene un factor primo.

Usando el tipo de lenguaje simbólico que acabamos de introducir, podríamos escribir esto en la forma:

Para todo x, $((E(x) \rightarrow P(x))$,

donde $E(x)$ simboliza «x es un entero» y $P(x)$ simboliza «x tiene un factor primo».

Análogamente, si introducimos símbolos de predicados H y M para simbolizar «es un hombre» y «es mortal», respectivamente, entonces «todos los hombres son mortales» puede escribirse:

Para todo x, $(H(x) \rightarrow M(x))$.

La frase «para todo x» se llama *cuantificador universal* y se simboliza como $(\forall x)$. Nótese que cuando escribimos $(\forall x)$ $(H(x) \rightarrow M(x))$ no suponemos nada acerca de la naturaleza del objeto x. La implicación se afirma «para todo objeto x del universo». Si x es un hombre entonces x es mortal, para todo x que no sea hombre, el si ese x particular es mortal o no es irrelevante. La implicación es verdadera porque su primera parte es falsa (véase la tabla de verdad de $\rightarrow$).

La introducción del símbolo x no debe causar confusión, pese a que no aparece en la frase castellana original. Su empleo no es más que una abreviatura matemática, y está claro que «todos los hombres son mortales» también puede simbolizarse como:

Para todo y, $(H(y) \rightarrow M(y))$.

Emplearemos las letras x e y como variables, como sujetos indeterminados. Cuando se usan, como más arriba, en enunciados que comienzan con cuantificadores, se llaman variables *ligadas*.

Hay otra clase de cuantificador que parece necesario a primera vista para simbolizar frases castellanas corrientes. Consideremos la frase: «Algunos cerdos tienen alas.» Una reformulación sería: «Existe al menos un cerdo que tiene alas», o bien, usando un artificio similar al de más arriba:

Existe al menos un objeto x tal que
x es un cerdo y x tiene alas.

La frase «existe al menos un objeto x tal que» se llama *cuantificador existencial* y se simboliza por $(\exists x)$. La frase puede escribirse ahora como

$$(\exists x)(C(x) \wedge A(x)),$$

donde $C(x)$ y $A(x)$ significan «x es un cerdo» y «x tiene alas», respectivamente.

Más en general, si A es un símbolo que representa un predicado,

tiene sentido escribir $(\forall x)A(x)$ y $(\exists x)A(x)$. Lo primero significa «todo objeto tiene la propiedad determinada por A», y lo segundo significa «existe algún objeto que tiene la propiedad determinada por A».

Ejemplo 3.2

Simbolícense:

(a) No todas las aves saben volar.
(b) Todo el mundo puede hacer eso.
(c) Algunas personas son estúpidas.
(d) Existe un entero que es mayor que cualquier otro entero.

Respuestas: (naturalmente, puede haber otras).

(a) $\sim(\forall x)(A(x)\rightarrow V(x))$.
(b) $(\forall x)(H(x)\rightarrow P(x))$.

Puede servir de ayuda el recorrer los pasos dados, como hicimos antes. «Todo el mundo puede hacer eso» significa «Todas las personas pueden hacer eso» y, al igual que antes, esto significa «Para todo x, si x es una persona, entonces x puede hacer eso». $H(x)$ simboliza «x es una persona» y $P(x)$ simboliza «x puede hacer eso».

(c) $(\exists x)(H(x) \wedge S(x))$.
(d) $(\exists x)(E(x) \wedge (\forall y)(E(y)\rightarrow x \geqslant y))$.

Veremos que estos ejemplos ilustran un esquema común, aunque no universal. El cuantificador universal va seguido muy frecuentemente de una implicación, debido a que los enunciados universales suelen ser de la forma «dado un x cualquiera, si tiene la propiedad A entonces tiene también la propiedad B».

Consideremos (a) con más detenimiento. Es bien sabido que se trata de una afirmación verdadera, que podemos justificar mediante los ejemplos de las avestruces, kiwis y pingüinos. Intuitivamente, justificamos «no todas las aves saben volar» justificando «existen aves que no saben volar». Aquí tenemos una importante conexión entre los dos cuantificadores, ya que un momento de reflexión bastará para convencernos de que los dos enunciados recién considerados tienen el mismo significado. Simbolicémoslos.

(i) $\sim(\forall x)(A(x)\rightarrow V(x))$,
(ii) $(\exists x)(A(x) \wedge \sim V(x))$.

Para comparar más de cerca, transformemos el primero en

$$\sim(\forall x)(\sim A(x) \vee V(x))$$

según las reglas del Capítulo 1, y luego en

$$\sim(\forall x)\sim(A(x) \wedge \sim V(x)).$$

La forma de este enunciado es ahora similar a la de (ii), pero con $\sim(\forall x)\sim$ en lugar de $(\exists x)$.

La consideración de ejemplos como éste nos permite comprender intuitivamente que las dos frases:

(i) No es el caso que todos los x no tengan la propiedad P,
(ii) Existe algún x que tiene la propiedad P,

tienen el mismo significado, cualquiera que sea la propiedad P.

Ejemplo 3.3

Simbolícense los enunciados siguientes, primeramente sin usar cuantificadores universales y después sin usar cuantificadores existenciales.

(*a*) Todas las aves saben volar.
(*b*) Ningún hombre es una isla.
(*c*) Algunos números no son racionales.

Respuestas:

(*a*) $\sim(\exists x)(A(x) \wedge \sim V(x))$
$(\forall x)(A(x) \rightarrow V(x))$.
(*b*) $\sim(\exists x)(H(x) \wedge I(x))$
$(\forall x)(H(x) \rightarrow I(x))$.
(*c*) $(\exists x)(N(x) \wedge \sim R(x))$
$\sim(\forall x)(N(x) \rightarrow R(x))$.

(Naturalmente, existen otras simbolizaciones equivalentes.)

▷Ahora que ya sabemos simbolizar, ¿cómo nos ayuda esto a decidir las relaciones entre enunciados o la validez de argumentaciones? No es posible extender el uso de las tablas de verdad, porque nuestros enunciados de ahora ya no tienen el carácter de funciones de verdad. El uso de variables y cuantificadores significa que el valor de verdad de una frase ya no depende simplemente de los valores de verdad de sus partes componentes, como era el caso antes; ni siquiera se da el caso de que las partes componentes tengan siempre valores de verdad. En particular, no tiene sentido hablar del valor de verdad de una parte de una frase que contenga una variable sin cuantificar, como por ejemplo «x es un ave», o $A(x)$, en el simbolismo del ejemplo anterior.

Ejercicios

1 Simbolícense las frases siguientes, empleando cuantificadores, variables y símbolos de predicado.
(*a*) No toda función tiene derivada.
(*b*) Existe una función que es continua pero no tiene derivada.
(*c*) Si algunos trenes se retrasan entonces todos los trenes se retrasan.
(*d*) Todo número es o par o impar.
(*e*) Ningún número es a la vez par e impar.
(*f*) Algunas personas odian a todo el mundo.
(*g*) Los elefantes son más pesados que los ratones.

2 Simbolícese cada uno de los enunciados siguientes, primeramente sin utilizar cuantificadores existenciales y después sin utilizar cuantificadores universales.
   (*a*) No todos los coches tienen tres ruedas.
   (*b*) Algunas personas son o perezosas o estúpidas.
   (*c*) Ningún ratón es más pesado que un elefante.
   (*d*) Todo número es negativo o posee raíz cuadrada.
3 Escójanse pares cualesquiera de enunciados de los Ejercicios 1 y 2 que tengan el mismo significado.

3.2 Lenguajes de primer orden

Un método de análisis de enunciados y argumentaciones es la lógica silogística. Esta materia tiene una larga genealogía, que se extiende desde Aristóteles hasta nuestros días. El lector interesado puede seguirla con más detalle en otros libros (por ejemplo, Copi), así que no entraremos en ello aquí. Se basa en el estudio de un pequeño número de formas argumentales particulares intuitivamente válidas, como por ejemplo la mencionada al comienzo de este capítulo:

Todos los *A*s son *B*
C es un *A*
$\therefore$ *C* es un *B*.

El propósito es, dada una argumentación particular, expresarla por medio de una o más de estas formas argumentativas básicas, demostrando así su validez. Los lógicos y matemáticos modernos han considerado que este método de análisis es demasiado restrictivo y han buscado un método diferente de análisis. Lo que se ha desarrollado, y lo que estudiaremos aquí, tiene el gran mérito matemático de conducir a nuevas y ricas áreas de estudio que ni siquiera se contemplan en la lógica silogística.

Vamos a construir un sistema formal. Se trata de un sistema formal más complicado que el del Capítulo 2, como era de esperar, pero está edificado sobre los mismos principios. Hemos de describir primero un lenguaje formal, dando el alfabeto de símbolos y las reglas de construcción de las fórmulas bien formadas. En esto nos guiaremos por la experiencia que hemos adquirido más arriba simbolizando frases ordinarias, ya que nuestro propósito es hacer el lenguaje formal de tal manera que las frases ordinarias puedan ser traducidas a fórmulas bien formadas, y reflejar las propiedades lógicas de las frases en propiedades de las *fbfs* del sistema. En este punto hemos de aclarar una vez más que los símbolos del lenguaje formal no han de tener más significado ni propiedades que los especificados dentro del propio sistema formal. En ocasiones pueden interpretarse de diferentes maneras, pero estas interpretaciones no son parte del sistema.

El alfabeto de símbolos es el siguiente:

$x_1, x_2, \ldots$	variables,
$a_1, a_2, \ldots$	constantes individuales,
$A_1^1, A_2^1, \ldots; A_1^2, A_2^2, \ldots; A_1^3, A_2^3, \ldots;$	letras de predicado,
$f_1^1, f_2^1, \ldots; f_1^2, f_2^2, \ldots; f_1^3, f_2^3, \ldots;$	letras de función,
$(,),,$	signos de puntuación,
$\sim, \rightarrow$	conectivas,
$\forall$	cuantificador.

Observaciones 3.4

(*a*) Las constantes individuales se incluyen para que tengamos en nuestro lenguaje fórmulas que puedan interpretarse como enunciados acerca de cosas particulares. Por ejemplo, el enunciado «Sócrates es un hombre» podría ser una interpretación de la fórmula $A_1^1(a_1)$.

(*b*) Hay una lista de listas de letras de predicado. La primera de ellas es una lista de letras de predicado monarias que están pensadas para representar predicados monarios (tales como «es un hombre»). La siguiente es una lista de letras de predicado binarias, para simbolizar relaciones o predicados binarios (tales como «es el padre de»). Y así sucesivamente. (Un ejemplo de predicado ternario en lenguaje ordinario es el enunciado «los puntos A, B y C son colineales».)

(*c*) No hemos visto letras que representen funciones en ninguna de las simbolizaciones informales que han aparecido hasta ahora. La idea de función es tan fundamental en matemáticas que resulta ventajoso admitir letras para funciones en el lenguaje formal. Esto es debido a que las interpretaciones de los símbolos que tenemos previstas son principalmente matemáticas. Naturalmente, una función es una clase especial de relación, y sería suficiente de hecho el disponer de símbolos para relaciones (letras de predicado), pero nuestro interés primordial no radica en achicar lo más posible el alfabeto de símbolos. Estamos aplicando también el criterio de claridad intuitiva. Más adelante, cuando discutamos sistemas matemáticos específicos, veremos con bastante claridad el efecto de la inclusión de letras de función, aptas para representar funciones de diferente número de argumentos. En ambos casos, el superíndice indica el número de argumentos.

(*d*) Hay un solo cuantificador en el lenguaje, el cuantificador universal. Hemos visto ya que el cuantificador existencial se puede definir en términos del cuantificador universal, de manera que sólo necesitamos tener uno de los dos. Por motivos análogos, incluimos a $\sim$ y $\rightarrow$ como únicas conectivas.

(*e*) Hay listas infinitas de símbolos, pese a que sólo admitiremos combinaciones finitas de éstos como fórmulas bien formadas (véase más abajo). Necesitamos un número *potencialmente* infinito de símbolos para mantener nuestro lenguaje lo más general posible. En las aplicaciones solamente especificaremos interpretaciones para algunos de estos símbolos, y algunas aplicaciones pueden necesitar más símbolos que otras, de manera que no nos interesa poner una cota superior al número de símbolos interpretables.

▷ En general, un *lenguaje de primer orden* $\mathscr{L}$ tendrá como alfabeto de símbolos:

variables $x_1, x_2, \ldots,$
algunas (eventualmente ninguna) de las constantes individuales $a_1, a_2, \ldots,$
algunas (eventualmente ninguna) de las letras de predicado A_i^n,
algunas (eventualmente ninguna) de las letras de función f_i^n,
los símbolos de puntuación (,) y ,,
las conectivas $\sim$ y $\rightarrow$,
el cuantificador $\forall$.

Está claro que existen muchos lenguajes de primer orden diferentes, dependiendo de los símbolos que se incluyan. En la mayor parte de nuestro trabajo no especificaremos qué lenguaje empleamos, por lo cual los resultados que obtengamos serán aplicables a todo lenguaje. El significado del término «primer orden» surgirá más tarde; está conectado con el uso del cuantificador universal.

Para especificar por completo un lenguaje de primer orden, hemos de decir lo que es una fórmula bien formada; pero consideremos primero algunos ejemplos.

Ejemplo 3.5

(*a*) Si queremos que nuestro lenguaje de primer orden sea apropiado para enunciados referentes a la aritmética de los números naturales, deberemos hacer que $\mathscr{L}$ contenga (junto con las variables, los signos de puntuación, las conectivas y el cuantificador) los símbolos:

a_1, para representar el 0,
A_1^2, para representar $=$,
f_1^1, para representar la función sucesor,
f_1^2, para representar $+$,
f_2^2, para representar $\times$.

Entonces, por ejemplo,

$$A_1^2(f_1^2(x_1, x_2), f_2^2(x_1, x_2))$$

se interpretaría como «$x_1 + x_2 = x_1 x_2$».

(*b*) Si queremos que nuestro lenguaje de primer orden sea apropiado para enunciados relativos a grupos, podemos tomar un $\mathscr{L}$ que contenga (junto con las variables, los signos de puntuación, las conectivas y el cuantificador) los símbolos:

a_1, para representar el elemento identidad,
A_1^2, para representar $=$,
f_1^1, para representar la función que transforma cada elemento en su inverso,
f_1^2, para representar la operación binaria del grupo.

Entonces, por ejemplo,

$$A_1^2(f_1^2(x_1, f_1^1(x_1)), a_1)$$

se interpretaría como «$x_1 \cdot x_1^{-1} =$ identidad».

Definición 3.6

Antes de definir las fórmulas bien formadas necesitamos algunos preliminares. Sea $\mathscr{L}$ un lenguaje de primer orden. *Término* de $\mathscr{L}$ se define del siguiente modo:

(i) Las variables y las constantes individuales son términos.
(ii) Si f_i^n es una letra de función de $\mathscr{L}$, y si $t_1, \ldots, t_n$ son términos de $\mathscr{L}$, entonces $f_i^n(t_1, \ldots, t_n)$ es un término de $\mathscr{L}$.
(iii) El conjunto de todos los términos es el generado por (i) e (ii).

Los términos van a ser aquellas expresiones del lenguaje formal que se interpretan como objetos, es decir, las cosas a las que se aplican las funciones, las cosas que tienen propiedades, las cosas acerca de las cuales se hacen aseveraciones.

Fórmula atómica de $\mathscr{L}$ se define así: Si A_j^k es una letra de predicado de $\mathscr{L}$ y $t_1, \ldots, t_k$ son términos de $\mathscr{L}$, entonces $A_j^k(t_1, \ldots, t_k)$ es una fórmula atómica de $\mathscr{L}$.

Las fórmulas atómicas son las expresiones más sencillas del lenguaje que son interpretables como aseveraciones, como por ejemplo que un cierto objeto verifica una cierta propiedad. La palabra «atómica» significa por supuesto «indivisible».

Las fórmulas atómicas, siguiendo la analogía que sugiere el término, son la materia de la que están hechas las fórmulas bien formadas.

Se pueden combinar de acuerdo con ciertas reglas lógicas y ocupan un lugar comparable al de las letras de enunciado en nuestro anterior sistema formal.

Fórmula bien formada de $\mathscr{L}$ se define por:
(i) Toda fórmula atómica de $\mathscr{L}$ es una *fbf* de $\mathscr{L}$.
(ii) Si $\mathscr{A}$ y $\mathscr{B}$ son *fbfs* de $\mathscr{L}$, también lo son $(\sim\mathscr{A})$, $(\mathscr{A}\rightarrow\mathscr{B})$ y $(\forall x_i)\,\mathscr{A}$, siendo x_i cualquier variable.
(iii) El conjunto de todas las *fbfs* de $\mathscr{L}$ es el generado por (i) e (ii).

Observación 3.7

(*a*) Las *fbfs* están construidas a partir de las fórmulas atómicas de la misma manera que en el sistema formal *L*, exceptuando, por supuesto, la inclusión del cuantificador universal. Si $\mathscr{A}$ es una *fbf* de $\mathscr{L}$, también lo es $(\forall x_i)\,\mathscr{A}$, siendo x_i cualquier variable. Así pues, por ejemplo, si $A_1^1(x_2)$ es una *fbf* de $\mathscr{L}$, también lo es $(\forall x_i)\,\mathscr{A}$, siendo x_i cualquier variable. Así pues, por ejemplo, si $A_1^1(x_2)$ es una *fbf* de $\mathscr{L}$, también lo es $(\forall x_1)\,A_1^1(x_2)$. Por tanto, no es necesario que el cuantificador tenga conexión con la *fbf* a la que se aplica, aunque evidentemente nos ocuparemos más de los casos en los que la variable cuantificada aparezca en la fórmula subsiguiente.

(*b*) Lo mismo que en el sistema *L*, incluimos solamente las conectivas $\sim$ y $\rightarrow$. Esto es con vistas a simplificar nuestras demostraciones de propiedades del lenguaje y de los sistemas formales basados en el lenguaje. Por la misma razón, excluimos el símbolo $\exists$. No obstante, más adelante nos resultará conveniente usar el símbolo $\exists$ y las conectivas $\wedge$ y $\vee$ como símbolos *definidos*, siguiendo las ideas intuitivas ya indicadas anteriormente.

$(\exists x_i)\,\mathscr{A}$ es una abreviatura de $(\sim((\mathscr{A}x_i)(\sim\mathscr{A})))$,
$(\mathscr{A}\wedge\mathscr{B})$ es una abreviatura de $(\sim(\mathscr{A}\rightarrow(\sim\mathscr{B})))$,
$(\mathscr{A}\vee\mathscr{B})$ es una abreviatura de $((\sim\mathscr{A})\rightarrow\mathscr{B})$.

Las fórmulas que incluyen estos símbolos no son estrictamente *fbfs* del lenguaje formal, pero pueden traducirse a *fbfs* de ser necesario.

(*c*) El uso de paréntesis en las fórmulas bien formadas se indica con precisión en la definición. No obstante, como ya hicimos en *L*, a veces omitiremos paréntesis, en tanto que ello no introduzca ambigüedades. Al igual que antes, se supondrá que un símbolo $\sim$ se aplica a la *fbf* subsiguiente más corta posible; por ejemplo, $(\sim\mathscr{A}\rightarrow\mathscr{B})$ es una abreviatura de $((\sim\mathscr{A})\rightarrow\mathscr{B})$. Trataremos los cuantificadores de manera similar; por ejemplo, $((\forall x_i)\mathscr{A}\rightarrow\mathscr{B})$ es una *fbf* en la que no se han omitido paréntesis; no deje de observarse la diferencia entre esta *fbf* y la *fbf* $(\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})$. Introduzcamos alguna terminología en relación con esto.

Definición 3.8

En la *fbf* $(\forall x_i)\,\mathscr{A}$, decimos que $\mathscr{A}$ es el *radio de acción* del cuantificador. Más en general, si $((\forall x_i)\,\mathscr{A})$ aparece como subfórmula de una *fbf* $\mathscr{B}$, decimos que el radio de acción de este cuantificador en $\mathscr{B}$ es $\mathscr{A}$.

Una intervención de la variable x_i en una *fbf* se dice que es *ligada* si la variable aparece dentro del radio de acción de un $(\forall x_i)$ en la *fbf*, o si es la x_i de un $(\forall x_i)$. Si una intervención de una variable no es ligada, se dice que es *libre*.

Ejemplo 3.9

(*a*) En la *fbf* $(\forall x_1)A_1^1(x_2)$ el radio de acción del cuantificador $(\forall x_1)$ es $A_1^1(x_2)$, la variable x_2 aparece libre, y la variable x_1 aparece ligada.

(*b*) $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2)\rightarrow A_1^1(x_2))$ es una *fbf* en la cual todas las intervenciones de x_1 y x_2 son ligadas. El radio de acción del $(\forall x_1)$ es $(\forall x_2)(A_1^2(x_1, x_2)\rightarrow A_1^1(x_2))$.

(*c*) $(\forall x_1)(A_1^2(x_1, x_2)\rightarrow(\forall x_2)A_1^1(x_2))$ es una *fbf* en la cual x_1 aparece ligada dos veces y x_2 aparece libre una vez y ligada dos veces. El radio de acción del $(\forall x_1)$ es $(A_1^2(x_1, x_2)\rightarrow(\forall x_2)A_1^1(x_2))$, y el radio de acción del $(\forall x_2)$ es $A_1^1(x_2)$.

▷ En lo anterior hemos estado usando símbolos que no son parte del lenguaje formal, concretamente $\mathscr{A}$ y $\mathscr{B}$. El lector recordará una situación similar en el Capítulo2. Estas letras son parte del lenguaje matemático ordinario que estamos usando para describir y discutir el formal, y pueden representar fórmulas bien formadas (generalmente arbitrarias) del lenguaje formal. A veces escribiremos también $\mathscr{A}(x_1)$ o $\mathscr{B}(x_1, ..., x_n)$, por ejemplo, cuando estemos interesados en ciertas variables (o términos) particulares. Estas expresiones indicarán a menudo, aunque no siempre, que las variables mencionadas aparecen libres en la *fbf*. Si x_i aparece libre en $\mathscr{A}(x_i)$, entonces, para todo término t, $\mathscr{A}(t)$ denotará el resultado de sustituir por t cada intervención libre de x_i.

Ejemplo 3.10

Examinaremos el uso de variables cuantificadas, volviendo a nuestro anterior ejemplo $(\forall x_1)A_1^1(x_2)$. Intuitivamente, la idea es que ésto se interprete como «sea cual sea el objeto x_1, la propiedad determinada por A_1^1 se verifica para el objeto representado por x_2». El cuantificador es claramente redundante, y otros cuantificadores puestos en el lugar de $(\forall x_1)$ serían redundantes también. $(\forall x_3)A_1^1(x_2)$ tendría la misma interpretación intuitiva, al igual que $(\forall x_7)A_1^1(x_2)$. No obstante, está claro que la interpretación intuitiva de $(\forall x_2)A_1^1(x_2)$ es esencialmente diferente de cualquiera de las anteriores. Sería «cualquiera que sea el objeto x_2, la propiedad determinada por A_1^1 se verifica para ese objeto». Y, sin necesidad de referirse a interpretaciones intuitivas; hay una diferen-

cia puramente formal entre $(\forall x_2) A_1^1(x_2)$ y los otros casos, consistente en que las dos variables que intervienen son la misma.

Muchas veces tendremos ocasión de reemplazar variables por otras variables o términos, y queremos hacerlo de manera que la interpretación intuitiva no varíe. Para utilizar el mismo ejemplo, $(\forall x_1) A_1^1(x_2)$: Si reemplazamos x_2 por x_3 obtenemos una *fbf* que tiene la misma forma de interpretación, y si reemplazamos x_2 por x_1 obtenemos una *fbf* que tiene una forma de interpretación diferente. Diremos que x_3 está libre para x_2 en $(\forall x_1) A_1^1(x_2)$, pero que x_1 no lo está. Más en general, si reemplazamos x_2 por el término $f_1^2(x_1, x_3)$, por ejemplo, obtenemos $(\forall x_1) A_1^1(f_1^2(x_1, x_3))$, y existe una interacción entre el cuantificador $(\forall x_1)$ y su radio de acción que no estaba presente previamente. Por ello, diremos que $f_1^2(x_1, x_3)$ no está libre para x_2 en $(\forall x_1) A_1^1(x_2)$. No obstante, un término en el que no aparezca la variable x_1 está libre para x_2 en $(\forall x_1) A_1^1(x_2)$. Extendamos estas ideas a una definición general.

Definición 3.11

Sea $\mathscr{A}$ una *fbf* arbitraria de $\mathscr{L}$. Un término t está *libre para* x_i en $\mathscr{A}$ si x_i no aparece libre en $\mathscr{A}$ dentro del radio de un $(\forall x_j)$, siendo x_j alguna de las variables que intervienen en t.

Esto viene a significar (del mismo modo, que más arriba) que t puede sustituirse en el lugar de cualquier intervención libre de x_i en $\mathscr{A}$ sin que aparezcan interacciones con cuantificadores de $\mathscr{A}$.

Ejemplo 3.12

Ya hemos visto algunos ejemplos más arriba. Uno más complicado es

$$((\forall x_1) A_1^2(x_1, x_2) \rightarrow (\forall x_3) A_2^2(x_3, x_1))$$

Aquí vemos, por ejemplo, que $f_1^2(x_1, x_4)$ no está libre para x_2, que $f_2^2(x_2, x_3)$ está libre para x_2, que x_2 está libre para x_1 (nótese que x_1 sólo aparece libre una vez) y que $f_4^2(x_1, x_3)$ no está libre para x_1.

Observación 3.13

Para toda *fbf* $\mathscr{A}$ y toda variable x_i (tanto si x_i aparece libre en $\mathscr{A}$ como si no), x_i está libre para x_i en $\mathscr{A}$.

▷ Hemos descrito el lenguaje formal que vamos a usar y desarrollar. Procederemos, lo mismo que en el Capítulo 2, a indicar axiomas y reglas de deducción para completar la especificación de diversos sistemas formales, que llamaremos sistemas del *Cálculo de Predicados de Primer Orden*. No obstante, antes de hacerlo es conveniente investigar la palabra «interpretación» que hemos usado ya vagamente varias veces, y tratar de precisarla.

Ejercicios

4 Sea $\mathscr{L}$ un lenguaje de primer orden cuyo alfabeto de símbolos no contenga letras de función. Descríbase el conjunto de términos de $\mathscr{L}$.

5 Descríbase el conjunto de términos del lenguaje de primer orden cuyo alfabeto de símbolos no contiene constantes individuales y tiene un único símbolo de función f_1^1.

6 ¿Cuáles de entre las siguientes son *fbfs*?
(*a*) $A_1^2(f_1^1(x_1), x_1)$.
(*b*) $f_1^3(x_1, x_3, x_4)$.
(*c*) $(A_1^1(x_2) \rightarrow A_1^3(x_3, a_1))$.
(*d*) $\sim(\forall x_2)A_1^2(x_1, x_2)$.
(*e*) $((\forall x_2)A_1^1(x_1) \rightarrow (\sim A_1^1(x_2)))$.
(*f*) $A_1^3(f_2^3(x_1, x_2, x_3))$.
(*g*) $(\sim A_1^1(x_1) \rightarrow A_1^1(x_2))$.
(*h*) $(\forall x_1)A_1^3(a_1, a_2, f_1^1(a_3))$.

7 ¿Cuáles de entre las apariciones de x_1 en las siguientes *fbfs* son libres, y cuáles son ligadas?
(*a*) $(\forall x_2)(A_1^2(x_1, x_2) \rightarrow A_1^2(x_2, a_1))$.
(*b*) $(A_1^1(x_3) \rightarrow (\sim(\forall x_1)(\forall x_2)A_1^3(x_1, x_2, a_1)))$.
(*c*) $((\forall x_1)A_1^1(x_1) \rightarrow (\forall x_2)A_1^2(x_1, x_2))$.
(*d*) $(\forall x_2)(A_1^1(f_1^2(x_1, x_2), x_1) \rightarrow (\forall x_1)A_2^2(x_3, f_2^2(x_1, x_2)))$.
¿Está el término $f_1^2(x_1, x_3)$ libre para x_2 en alguna de las *fbfs* anteriores?

8 Sea $\mathscr{A}(x_i)$ una *fbf* de $\mathscr{L}$ en la que aparece libre x_i, y sea x_j una variable que no aparece libre en $\mathscr{A}(x_i)$. Demuéstrese que si x_j está libre para x_i en $\mathscr{A}(x_i)$, entonces x_i está libre para x_j en $\mathscr{A}(x_j)$. $\mathscr{A}(x_j)$ es el resultado de sustituir cada intervención libre de x_i en $\mathscr{A}(x_i)$ por x_j.

9 En cada uno de los casos siguientes, sea $\mathscr{A}(x_1)$ la *fbf* dada, y sea t el término $f_1^2(x_1, x_3)$. Escríbase la *fbf* $\mathscr{A}(t)$, decidiendo en cada caso si t está libre para x_1 en la *fbf* dada.
(*a*) $((\forall x_2)A_1^2(x_2, f_1^2(x_1, x_2)) \rightarrow A_1^1(x_1))$.
(*b*) $(\forall x_1)(\forall x_3)(A_1^1(x_3) \rightarrow A_1^1(x_1))$.
(*c*) $(\forall x_2)A_1^1(f_1^1(x_2)) \rightarrow (\forall x_3)A_1^3(x_1, x_2, x_3)$.
(*d*) $(\forall x_2)A_1^3(x_1, f_1^1(x_1), x_2) \rightarrow (\forall x_3)A_1^1(f_1^2(x_1, x_3))$.

10 Repítase el Ejercicio 9 para los siguientes términos t.
(*a*) x_2.
(*b*) x_3.
(*c*) $f_1^2(a_1, x_1)$.
(*d*) $f_1^3(x_1, x_2, x_3)$.

3.3 Interpretaciones

Definición 3.14

Una interpretación I para $\mathscr{L}$ es un conjunto no vacío D_I (el *dominio* de I) junto con una colección de elementos distinguidos $(\bar{a}_1, \bar{a}_2, \ldots)$, una colección de funciones sobre $D_I(\bar{f}_i^n,\ i>0,\ n>0)$, y una colección de relaciones sobre $D_I(\bar{A}_i^n,\ i>0,\ n>0)$.

▷ Ya se ha señalado anteriormente que las variables $x_1, x_2, \ldots$ de $\mathscr{L}$ estaban destinadas a interpretarse como «objetos». El conjunto D_I pretende ser el dominio de objetos sobre el que se supone que varían las variables. La colección de elementos distinguidos constará de objetos particulares que se suponen simbolizados por las constantes individuales. Análogamente, las relaciones y funciones se consideran interpretaciones concretas de las letras de predicado y las letras de función de $\mathscr{L}$. Nótese que para un lenguaje particular $\mathscr{L}$, las litas de constantes, letras de función y letras de predicado pueden estar restringidas. Una interpretación para un tal lenguaje $\mathscr{L}$ tendrá tan sólo los elementos distinguidos, funciones y relaciones necesarios para interpretar los símbolos de $\mathscr{L}$.

Ahora estamos en condiciones de aclarar el término «lenguaje de primer orden». Un lenguaje así contiene variables interpretables como objetos del dominio de interpretación, y cuantificadores referidos a dichas variables. Así pues, en una interpretación los cuantificadores varían sobre objetos del dominio. Esta es la propiedad característica de un lenguaje de primer orden. Un lenguaje de segundo orden contendría además cuantificadores interpretables como referidos a variables que varíen sobre relaciones entre (y, por tanto, conjuntos de) objetos del dominio de la interpretación. Un lenguaje así tendría dos clases de variables, una para objetos y otra para relaciones. Nosotros vamos a limitar enteramente nuestra atención a lenguajes y sistemas formales de primer orden.

Ejemplo 3.15

Aritmética Formal. Véase el Ejemplo 3.5(*a*), donde se describe el lenguaje de primer orden apropiado. Este contiene a_1, A_1^2, f_1^1, f_2^2, además de variables, signos de puntuación, conectivas y cuantificador. Podemos definir una interpretación N como sigue: Sea $D_N = \{0, 1, 2, \ldots\}$ el conjunto de los números naturales. El único elemento distinguido es el 0 (la interpretación de la constante individual a_1). La adición y la multiplicación de números naturales son las interpretaciones de las otras dos letras de función binaria f_1^2 y f_2^2, respectivamente, y la función sucesor es la interpretación de f_1^1. La relación $=$ es la interpretación de la letra de predicado A_1^2.

Mediante la interpretación anterior, las fórmulas bien formadas de este lenguaje pueden interpretarse como enunciados referentes a números naturales. Por ejemplo, la *fbf*.

$$(\forall x_1)(\forall x_2) \sim (\forall x_3)(\sim A_1^2(f_1^2(x_1, x_3), x_2)) \qquad (*)$$

tiene la interpretación

para todo x e $y \in D_N$, no es cierto que
para todo $z \in D_N$, $x + z \neq y$

o, equivalentemente

para todo x e $y \in D_N$, existe $z \in D_N$ tal que $x + z = y$

▷ Un ejemplo de un enunciado sobre números naturales que no es la interpretación de alguna *fbf* del lenguaje de primer orden apropiado es: «todo conjunto no vacío de números naturales tiene un elemento mínimo». Este enunciado comienza con un cuantificador universal sobre conjuntos de números y correspondería a una *fbf* de un lenguaje formal de *segundo* orden para la aritmética.

Solamente cuando se ha dado una interpretación de los símbolos de $\mathscr{L}$ tiene sentido hablar de *significados* de *fbfs*, y por lo tanto sólo podemos considerar la verdad y la falsedad en el contexto de una interpretación. La *fbf* (*) de más arriba resulta tener un significado falso en esta interpretación, pero en otras interpretaciones su significado bien pudiera ser verdadero.

Ejemplo 3.16

La *fbf* (*) tiene un significado verdadero en la interpretación I, siendo D_I el conjunto de los números racionales positivos, 1 la interpretación de a_1, e interpretándose f_1^2 como la multiplicación y f_2^2 como la división (función que calcula el cociente).

(*) se traduce en I como:
para todo x, $y \in D_I$ existe $z \in D_I$ tal que $x \cdot z = y$

Esta es una propiedad bien conocida de los números racionales.

▷ Hemos incluido este último ejemplo con el principal propósito de ilustrar que puede haber interpretaciones del mismo lenguaje formal $\mathscr{L}$ que difieran sustancialmente. En nuestros ejemplos de lenguajes, generalmente tendremos in mente alguna interpretación particular, pero esto no debe impedirnos el considerar otras interpretaciones y las consecuencias de su existencia.

Podemos ver ahora una similaridad entre esta situación y la situación del Capítulo 2. Allí, las *fbfs* del sistema L del cálculo de enunciados no podían considerarse en sí mismas como verdaderas o falsas. Verdad y falsedad eran relevantes tan sólo cuando asignábamos valores de verdad a las variables de enunciado o construíamos una valoración. Es más, vimos que algunas *fbfs* podían ser verdaderas o falsas, dependiendo de la valoración. En nuestro sistema actual, más complicado, la noción de interpretación corresponde a la asignación de valores de verdad. Una cuestión obvia a plantear ahora es: ¿Tenemos un análogo de las tautologías? La respuesta es «sí», y la definición es justamente la que sería de esperar, pero volveremos a considerar este punto más tarde. Ahora hemos de precisar más la idea de *verdad* con

respecto a una interpretación. A pesar de la aparente complejidad de lo que sigue, las ideas no son difíciles, y el lector deberá procurar tener presente el esbozo intuitivo que hemos construido ya. Para el resto de este capítulo, se sugiere que el lector no familiarizado con la materia omita los detalles de las demostraciones en una primera lectura. Las demostraciones no son importantes para la compresión intuitiva de las ideas implicadas, y éstas podrían verse oscurecidas por una atención excesiva a los detalles.

Ejercicios

11 Sea $\mathscr{L}$ el lenguaje de primer orden que incluye (junto con las variables, signos de puntuación, conectivas y cuantificador) la constante individual a_1, la letra de función f_1^2 y la letra de predicado A_2^2. Denotaremos por $\mathscr{A}$ la *fbf*.

$$(\forall x_1)(\forall x_2)(A_2^2(f_1^2(x_1,\ x_2),\ a_1)\rightarrow A_2^2(x_1,\ x_2))$$

Definamos una interpretación I para $\mathscr{L}$ como sigue. D_I es $\mathbb{Z}$, $\bar{a}_1$ es 0, $\bar{f}_1^2(x,\ y)$ es $x-y$, $\bar{A}_2^2(x,\ y)$ es $x<y$. Escríbase la interpretación de $\mathscr{A}$ en I. ¿Es un enunciado verdadero o falso? En cuéntrese otra interpretación en la cual $\mathscr{A}$ sea un enunciado con el valor de verdad opuesto.

12 ¿Existe una interpretación (para un lenguaje de primer orden $\mathscr{L}$ adecuado) en la cual la *fbf*

$$(\forall x_1)(A_1^1(x_1)\rightarrow A_1^1(f_1^1(x_1)))$$

se interprete como un enunciado falso? Si es así, escríbase una en detalle. En otro caso, explíquese por qué no existe.

13 Repítase el Ejercicio 12 con la *fbf*

$$(\forall x_1)(A_1^2(x_1,\ x_2)\rightarrow A_1^2(x_2,\ x_1))$$

3.4 Satisfacción, verdad

Sea I una interpretación para el lenguaje $\mathscr{L}$, de dominio D_I. Aquí y en lo que sigue usaremos la notación de la Definición 3.14. Las interpretaciones en I de a_i, f_i^n, A_i^n se denotarán por $\bar{a}_i$, $\bar{f}_i^n$, $\bar{A}_i^n$, respectivamente. Nótese que, para cada i, $\bar{a}_i \in D_I$, $\bar{f}_i^n\colon D_I^n \rightarrow D_I$ y $\bar{A}_i^n$ es una relación n-aria sobre D_I.

Definición 3.17

Se llama *valoración* en I a toda función v del conjunto de términos de $\mathscr{L}$ en el conjunto D_I, que verifique las propiedades:

(i) $v(a_i)=\bar{a}_i$ para toda constante individual a_i de $\mathscr{L}$.

(ii) $v(f_i^n(t_1, \ldots, t_n))=\bar{f}_i^n(v(t_1), \ldots, v(t_n))$, siendo f_i^n cualquier letra de función de $\mathscr{L}$, y $t_1, \ldots, t_n$ términos cualesquiera de $\mathscr{L}$

Una valoración no es más que una regla que asigna a cada término de $\mathscr{L}$ el objeto de D_I destinado a ser su interpretación. La parte (ii) asegura la consistencia de la regla.

Observaciones 3.18

(*a*) En general, en una interpretación dada existirán diferentes valoraciones.

b) Una valoración v queda completamente especificada indicando lo valores de $v(x_1)$, $v(x_2)$, ... Esto es debido a que los $v(a_i)$ vienen dados por la definición (*i*), e, inductivamente, para todo término $f_i^n(t_1, ..., t_n)$, el valor de $v(f_i^n(t_1, ..., t_n))$ viene determinado por (ii).

▷ Más tarde tendremos ocasión de manejar valoraciones casi idénticas, en el sentido siguiente.

Definición 3.19

Dos valoraciones v y v' son *i-equivalentes* si $v(x_j) = v'(x_j)$ para todo $j \neq i$.

Las valoraciones *i*-equivalentes asignan los mismos valores a todas las variables, excepto quizá x_i; pero nótese que, en general, los valores de términos en los que aparezca x_i diferirán.

▷ Consideremos ahora una *fbf* $\mathscr{A}$ de $\mathscr{L}$. Una valoración dada puede tener el efecto de «asignar un valor de verdad» a $\mathscr{A}$ del siguiente modo: Se reemplaza cada término t que aparezca en $\mathscr{A}$ por $v(t)$, y cada letra de función y de predicado por su interpretación en I. Lo que se obtiene es un enunciado acerca de los elementos del conjunto D_I, que puede ser verdadero o falso. Si es verdadero, se dice que v satisface $\mathscr{A}$.

Precisamos esto de la manera siguiente:

Definición 3.20

Sea $\mathscr{A}$ una *fbf* de $\mathscr{L}$, y sea I una interpretación para $\mathscr{L}$. Se dice que la valoración v en I *satisface* a la *fbf* $\mathscr{A}$ si puede demostrarse inductivamente que lo hace, a partir de las cuatro condiciones siguientes:

(i) v satisface la fórmula atómica $A_j^n(t_1, \ldots, t_n)$ si $\overline{A}_j^n(v(t_1), \ldots, v(t_n))$ se verifica en D_I.
(ii) v satisface $(\sim\mathscr{B})$ si v no satisface $\mathscr{B}$.
(iii) v satisface $(\mathscr{B}\rightarrow\mathscr{C})$ si v satisface $(\sim\mathscr{B})$ o v satisface $\mathscr{C}$.
(iv) v satisface $(\forall x_i)\,\mathscr{B}$ si toda valoración v' que sea *i*-equivalente a v satisface $\mathscr{B}$.

Observaciones 3.21

(*a*) Para v y $\mathscr{A}$ cualesquiera, o v satisface $\mathscr{A}$ o v satisface $(\sim\mathscr{A})$.

(*b*) Quizá sea necesario explicar un poco (iv). $(\forall x_i)\,\mathscr{B}$ se interpretará como un cierto enunciado del tipo «para todo $y \in D_I$, ...,», donde imaginamos a y como interpretación de x_i. v proporciona interpretaciones para las variables que aparecen en $\mathscr{B}$, y es razonable decir que v satisface $(\forall x_i)\,\mathscr{B}$ si, ante todo, v satisface $\mathscr{B}$ y si, además, cualquier otra valoración que se obtenga de v cambiando el valor de $v(x_i)$ también satisface $\mathscr{B}$.

(*c*) Puede servir de ayuda para la comprensión de esta definición el señalar que cada una de las cláusulas (i)-(iv) de más arriba puede considerarse como un enunciado «si y sólo si», por tener la naturaleza de una definición.

Ejemplo 3.22

(*a*) En la interpretación aritmética N, consideremos la *fbf* $A_1^2(f_1^2(x_1, x_2), f_2^2(x_3, x_4))$. Toda valoración v en la cual $v(x_1)=2$, $v(x_2)=6$, $v(x_3)=3$, $v(x_4)=4$ satisfacerá a esta *fbf*, puesto que $2\times 6=3\times 4$ es verdadero en D_N. Análogamente, ninguna valoración w que cumpla $w(x_1)=1$, $w(x_2)=5$, $w(x_3)=4$, $w(x_4)=2$ la satisfacerá.

(*b*) La *fbf* $(\forall x_1)A_1^2(f_2^2(x_1, x_2), f_2^2(x_2, x_1))$ se interpreta en N como «para todo $n \in D_N$, $nm=mn'$, que ciertamente se considerará como verdadero. Sea v una valoración en N. Entonces $v(x_1)$ y $v(x_2)$ son números naturales y $A_1^2(f_2^2(x_1, x_2), f_2^2(x_2, x_1))$ se interpreta como $v(x_1)\times v(x_2)=v(x_2)\times v(x_1)$, que es verdadero. Así pues, v satisface $A_1^2(f_2^2(x_1, x_2), f_2^2(x_2, x_1))$. Es más, si cambiamos el valor de $v(x_1)$ para obtener una nueva valoración 1-equivalente v', es fácil ver que v' también satisface $A_1^2(f_2^2(x_1, x_2), f_2^2(x_2, x_1))$. Así pues, por (iv) de la definición de más arriba, v satisface $(\forall x_1)A_1^2(f_2^2(x_1, x_2), F_2^2(x_2, x_1))$ en N. Por lo tanto, toda valoración v en N satisface esta *fbf*.

(*c*) La *fbf* $(\forall x_1)\,A_1^2(x_1, a_1)$ se interpreta intuitivamente como «para todo $n \in D_N$, $n=0'$, que es falsa. Sea v una valoración en N. Entonces $A_1^2(x_1, a_1)$ se interpreta por «$v(x_1)=0$». Así pues, v no satisface $A_1^2(x_1, a_1)$ salvo si $v(x_1)=0$. Supongamos que $v(x_1=0$, y preguntémonos si v satisface $(\forall x_1)A_1^2(x_1, a_1)$. Para que esto se cumpla, tendremos que estar en condiciones de asegurar que toda v' obtenida a partir de v cambiando el valor de $v(x_1)$ satisface también $A_1^2(x_1, a_1)$. Pero evidentemente no podemos asegurarlo. Por lo tanto, ninguna valoración en N satisface $(\forall x_1)\,A_1^2(x_1, a_1)$.

▷La sustitución de variables o términos en lugar de variables es una técnica que será importante más adelante. La siguiente proposición va a ser necesaria, pese a que su naturaleza técnica hace complicada la

demostración, que sirve de ilustración de la forma que van a asumir las demostraciones en esta parte de la materia.

Proposición 3.23

Sea $\mathscr{A}(x_i)$ una *fbf* de $\mathscr{L}$ en la que aparece libre x_i, y sea t un término que está libre para x_i en $\mathscr{A}(x_i)$. Supongamos que v es una valoración y que v' es la valoración i-equivalente a v y tal que $v'(x_i) = v(t)$. Entonces v satisface $\mathscr{A}(t)$ si y sólo si v' satisface $\mathscr{A}(x_i)$.

Demostración: Observamos primero que para todo término u en el que aparezca x_i podemos obtener otro término u' sustituyendo todas las intervenciones de x_i por t, y que entonces $v(u') = v'(u)$. Demostramos esto por inducción sobre la longitud de u, (por ejemplo, el número de símbolos que aparecen en u).

Paso base: u es x_i, de modo que u' es t. Entonces:

$$\begin{aligned} v'(u) &= v'(x_i) = v(t), \text{ (por definición de } v'), \\ &= v(u'). \end{aligned}$$

Paso de inducción: u es $f_i^n(u_1, \ldots, u_n)$, siendo $u_1, \ldots, u_n$ términos de longitud menor. Sean $u'_1, \ldots, u'_n$ los términos obtenidos sustituyendo cada intervención de x_i por t. Entonces $u' = f_i^n(u'_1, \ldots, u'_n)$. Así,

$$\begin{aligned} v(u') &= f_i^n(v(u'_1), \ldots, v(u'_n)) \\ &= f_i^n(v'(u_1), \ldots, v'(u_n)), \end{aligned}$$

por la hipótesis de inducción,

$$= v'(u).$$

Así pues, queda demostrado $v(u') = v'(u)$, para todo término u de $\mathscr{L}$.

Demostramos ahora la proposición por inducción sobre la longitud de la *fbf* $\mathscr{A}(x_i)$, es decir, el número de conectivas y cuantificadores de $\mathscr{A}(x_i)$.

Paso base: $\mathscr{A}(x_i)$ es una fórmula atómica, digamos $A_j^n(u_1, \ldots, u_n)$, siendo $u_1, \ldots, u_n$ términos de $\mathscr{L}$. Supongamos que v' satisface $\mathscr{A}(x_i)$. Entonces

$\overline{A}_j^n(v'(u_1), \ldots, v'(u_n))$ se verifica en la interpretación,

de modo que

$\overline{A}_j^n(v(u'_1), \ldots, v(u'_n))$ se verifica en la interpretación,

donde $u'_1, \ldots, u'_n$ se han obtenido como más arriba, sustituyendo cada intervención de x_i por t. (Aquí usamos el resultado preliminar de más arriba.) Tenemos ahora que v satisface la *fbf* $A_j^n(u'_1, \ldots, u'_n)$, es decir, v

satisface $\mathscr{A}(t)$. El recíproco puede demostrarse invirtiendo esta argumentación.

Paso de inducción:

Caso 1: $\mathscr{A}(x_i)$ es $(\sim\mathscr{B}(x_i))$
Caso 2: $\mathscr{A}(x_i)$ es $(\mathscr{B}(x_i)\rightarrow\mathscr{C}(x_i))$.

Estos casos son inmediatos y se dejan como ejercicio.

Caso 3: $\mathscr{A}(x_i)$ es $(\forall x_j)\mathscr{B}(x_i)$ $\quad (j\neq i)$

Supongamos que v no satisface $\mathscr{A}(t)$. Demostremos que v' no satisface $\mathscr{A}(x_i)$. Existe una valoración w que es j-equivalente a v y que no satisface $\mathscr{B}(t)$. Sea w' la valoración que es i-equivalente a w y cumple $w'(x_i)=w(t)$. Entonces, por la hipótesis de inducción aplicada a $\mathscr{B}(x_i)$, tenemos que w' no satisface $\mathscr{B}(x_i)$ (ya que w no satisface $\mathscr{B}(t)$.) Ahora bien, t está libre para x_i en $(\forall x_j)\mathscr{B}(x_i)$, así que x_j no aparece en t. Así pues, $v(t)$ depende sólo de los $v(x_k)$ para $k\neq j$. Pero para $k\neq j$, $v(x_k)=w(x_k)$, así que $v(t)=w(t)$. Se deduce que w' es j-equivalente a v', ya que w es j-equivalente a v. Ahora, como w' no satisface $\mathscr{B}(x_i)$, v' no satisface $(\forall x_j)\mathscr{B}(x_i)$, es decir, v' no satisface $\mathscr{A}(x_i)$. El recíproco requiere una argumentación similar y se deja como ejercicio.

Definición 3.24

Una *fbf* $\mathscr{A}$ es *verdadera* en una interpretación I si toda valoración en I satisface $\mathscr{A}$. $\mathscr{A}$ es *falsa* si no existe ninguna valoración en I que satisfaga $\mathscr{A}$.

Notación: Escribiremos $I\models\mathscr{A}$ si $\mathscr{A}$ es verdadera en I. Este símbolo no debe confundirse con $\vdash$; el lector notará que ninguno de ellos es un símbolo del lenguaje formal. Ambos son parte del metalenguaje que usamos para hablar de nuestros lenguajes formales.

Observaciones 3.25

(*a*) Puede ocurrir que para cierta *fbf* $\mathscr{A}$, algunas valoraciones en I satisfagan $\mathscr{A}$ y otras no. Una *fbf* así no es ni verdadera ni falsa en I.

(*b*) El dominio de una interpretación es por definición no vacío, así que, trivialmente, el conjunto de valoraciones no puede ser vacío. Está claro a partir de la definición que una valoración dada o satisface o no satisface una *fbf* $\mathscr{A}$ dada, y por lo tanto es imposible que una *fbf* sea a la vez verdadera y falsa en una interpretación dada.

(*c*) En una interpretación dada, una *fbf* $\mathscr{A}$ es falsa si y sólo si $(\sim\mathscr{A})$ es verdadera. Esto es una consecuencia inmediata de las definiciones de valoración y verdad. Se deduce que para ninguna *fbf* $\mathscr{A}$ puede ocurrir que $\mathscr{A}$ y $(\sim\mathscr{A})$ sean ambas verdaderas.

(*d*) En una interpretación dada I, una *fbf* $(\mathscr{A} \rightarrow \mathscr{B})$ es falsa si y sólo si $\mathscr{A}$ es verdadera y $\mathscr{B}$ es falsa. Demostremos uno de los dos sentidos, para ilustrar el modo en que se aplican las definiciones. Supongamos que $(\mathscr{A} \rightarrow \mathscr{B})$ es falsa en I. Entonces ninguna valoración satisface $(\mathscr{A} \rightarrow \mathscr{B})$ en I. Dada cualquier valoración v, tendremos que v no satisface $(\mathscr{A} \rightarrow \mathscr{B})$. Por la Definición 3.20(iii), v no satisface $(\sim \mathscr{A})$ y v no satisface $\mathscr{B}$. Así pues, v satisface $\mathscr{A}$ y v no satisface $\mathscr{B}$. Por lo tanto, toda valoración satisface $\mathscr{A}$ y no satisface $\mathscr{B}$. Se deduce que $\mathscr{A}$ es verdadera y que $\mathscr{B}$ es falsa.

Proposición 3.26

Si las *fbfs* $\mathscr{A}$ y $(\mathscr{A} \rightarrow \mathscr{B})$ son verdaderas en una interpretación particular I, entonces $\mathscr{B}$ es verdadera también.

Demostración: Sea v una valoración en I. Entonces v satisface $\mathscr{A}$ y v satisface $(\mathscr{A} \rightarrow \mathscr{B})$. Por la definición de satisfacción, se tiene entonces que v satisface $(\sim \mathscr{A})$ o v satisface $\mathscr{B}$. Pero v no puede satisfacer $(\sim \mathscr{A})$, así que v tiene que satisfacer $\mathscr{B}$. Se deduce que $\mathscr{B}$ es satisfecha por toda valoración en I, así que $\mathscr{B}$ es verdadera en I.

Proposición 3.27

Sea $\mathscr{A}$ una *fbf* de $\mathscr{L}$ y sea I una interpretación para $\mathscr{A}$. Entonces, $I \models \mathscr{A}$ si y sólo si $I \models (\forall x_i)\mathscr{A}$, siendo x_i cualquier variable.

Demostración: Supongamos que $I \models \mathscr{A}$, y sea v cualquier valoración en I. Entonces v satisface $\mathscr{A}$ y toda v' que sea i-equivalente también satisface $\mathscr{A}$, ya que toda valoración satisface $\mathscr{A}$. Así pues, v satisface $(\forall x_i)\mathscr{A}$, con lo que toda valoración satisface $(\forall x_i)\mathscr{A}$, p.e. $I \models (\forall x_i)\mathscr{A}$.

Supongamos ahora que $I \models (\forall x_i)\mathscr{A}$, y sea v cualquier valoración en I. v satisface entonces $(\forall x_i)\mathscr{A}$. Así pues, toda v' que sea i-equivalente a v satisface $\mathscr{A}$. En particular, v satisface $\mathscr{A}$, con lo que toda valoración satisface $\mathscr{A}$, es decir, $I \models \mathscr{A}$.

Corolario 3.28

Sean $y_1, \ldots, y_n$ variables de $\mathscr{L}$, sea $\mathscr{A}$ una *fbf* de $\mathscr{L}$, y sea I una interpretación. Entonces $I \models \mathscr{A}$ si y sólo si $I \models (\forall y_1) \ldots (\forall y_n)\mathscr{A}$.

Demostración: Por aplicación repetida de la proposición 3.27.

▷ Hay dos aspectos de este resultado que merecen mención. En primer lugar, el añadir un cuantificador para una variable que no aparece libre en $\mathscr{A}$, formando $(\forall x_i)\mathscr{A}$, no cambia la interpretación desde el punto de vista intuitivo (véase el Ejemplo 3.10), de manera que no hemos

de sorprendernos de que en estas circunstancias $\mathscr{A}$ sea verdadera si y sólo si $(\forall x_i)\mathscr{A}$ es verdadera. El añadir un cuantificador para una variable que aparece libre en $\mathscr{A}$, formando $(\forall x_i)\mathscr{A}(x_i)$, tiene diferente efecto; pero el resultado de más arriba indica que $\mathscr{A}(x_i)$ es verdadera si y sólo si $(\forall x_i)\mathscr{A}(x_i)$ es verdadera. De este modo, cuando consideramos la verdad o falsedad de *fbfs* con variables libres, el (los) cuantificador(es) universal(es) se sobreentiende(n) en un cierto sentido.

El cuantificador existencial se ha introducido como símbolo definido del lenguaje formal. Veamos cómo encaja en el contexto de las valoraciones y la satisfacción.

Proposición 3.29

En una interpretación I, una valoración v satisface la fórmula $(\exists x_i)\mathscr{A}$ si y sólo si existe al menos una valoración v' que es i-equivalente a v y que satisface $\mathscr{A}$.

Demostración: $(\exists x_i)\mathscr{A}$ es $\sim(\forall x_i)(\sim\mathscr{A})$. Supongamos que v satisface $\sim(\forall x_i)(\sim\mathscr{A})$. Entonces v no satisface $(\forall x_i)(\sim\mathscr{A})$. Así pues, existe alguna v' que es i-equivalente a v y no satisface $(\sim\mathscr{A})$. Esta v' debe forzosamente satisfacer $\mathscr{A}$. El recíproco se demuestra invirtiendo la argumentación.

▷El lenguaje del cálculo de proposiciones contenía las conectivas $\sim$ y $\rightarrow$. El lenguaje $\mathscr{L}$ las contiene también. Por lo tanto, si tomamos una *fbf* $\mathscr{A}_0$ de L y reemplazamos cada letra de enunciado que aparezca en ella por una *fbf.* de $\mathscr{L}$ (haciendo el mismo reemplazamiento para todas las intervenciones de una misma letra de enunciado), obtendremos una *fbf* $\mathscr{A}$ de $\mathscr{L}$. Se dice entonces que $\mathscr{A}$ *procede de* $\mathscr{A}_0$ *por sustitución.* Análogamente, partiendo de una *fbf.* de $\mathscr{L}$, podemos ver que tiene la misma estructura que alguna (generalmente varias) *fbfs* de L. Por ejemplo, consideremos

$$(\sim(\forall x_1)A_1^1(x_1)\rightarrow((\forall x_2)A_2^2(x_1,\ x_2)\rightarrow(A_1^1(x_2)\rightarrow(\forall x_1)A_3^1(x_1)))).$$

Esta *fbf.* proviene por sustitución de la *fbf* $(\sim p_1\rightarrow p_2)$ de L, y también de $(\sim p_1\rightarrow(p_2\rightarrow p_3))$. Otro ejemplo puede ser la *fbf.*

$$((\forall x_1)A_1^1(x_1)\rightarrow(\forall x_1)A_1^1(x_1))$$

que procede por sustitución de la *fbf* $(p_1\rightarrow p_1)$ de L. Ahora bien, $(p_1\rightarrow p_1)$ es una tautología. Extenderemos la noción de tautología a *fbfs* de $\mathscr{L}$ como sigue:

Definición 3.30

Una *fbf* $\mathscr{A}$ de $\mathscr{L}$ es una tautología si proviene por sustitución de una tautología de L.

Proposición 3.31

Una *fbf* de $\mathscr{L}$ que sea una tautología es verdadera en cualquier interpretación para $\mathscr{L}$.

Demostración: La analogía entre las Definiciones 2.12 y 3.30 es la que nos proporciona nuestro método. Sea $\mathscr{A}$ una *fbf* de $\mathscr{L}$ que proviene por sustitución de una *fbf* $\mathscr{A}_0$ de L. A partir de toda valoración v en una interpretación I podemos obtener una valoración (parcial) v' de L como sigue. Sean $p_1, \ldots, p_k$ las letras de enunciado que aparecen en $\mathscr{A}_0$, y sean $\mathscr{A}_1, \ldots, \mathscr{A}_k$ las *fbfs* de $\mathscr{L}$ que se han sustituido en lugar de ellas para obtener $\mathscr{A}$. Para $1 \leqslant i \leqslant k$, sea

$$v'(p_i) = \begin{cases} V \text{ si } v \text{ satisface } \mathscr{A}_i. \\ F \text{ si } v \text{ no satisface } \mathscr{A}_i. \end{cases}$$

Demostramos ahora que v satisface $\mathscr{A}$ si y sólo si $v'(\mathscr{A}_0) = V$. La demostración tiene lugar por inducción sobre el número de conectivas de $\mathscr{A}_0$.

Paso base: $\mathscr{A}_0$ es una letra de enunciado, por ejemplo, p_n. Por la definición de v', tenemos entonces que $v'(p_n) = V$ si y sólo si v satisface $\mathscr{A}$.

Paso de inducción:

Caso 1: $\mathscr{A}_0$ es $\sim\mathscr{B}_0$, con lo que $\mathscr{A}$ es $\sim\mathscr{B}$, donde $\mathscr{B}$ proviene de $\mathscr{B}_0$ por sustitución. Por la hipótesis de inducción, v satisface $\mathscr{B}$ si y sólo si $v'(\mathscr{B}_0) = V$. Así pues, v no satisface $\mathscr{B}$ si y sólo si $v'(\mathscr{B}_0) = F$. Se deduce que v satisface $\mathscr{A}$ si y sólo si $v'(\mathscr{A}_0) = V$, usando las definiciones 3.20(ii) y 2.12(i).

Caso 2: $\mathscr{A}_0$ es $(\mathscr{B}_0 \rightarrow \mathscr{C}_0)$, por lo que $\mathscr{A}$ es $(\mathscr{B} \rightarrow \mathscr{C})$, donde $\mathscr{B}$ y $\mathscr{C}$ provienen por sustitución de $\mathscr{B}_0$ y $\mathscr{C}_0$, respectivamente. Las afirmaciones siguientes son todas equivalentes:

(*a*) v satisface $\mathscr{A}$.
(*b*) o v satisface $\sim\mathscr{B}$ o v satisface $\mathscr{C}$ (por la Definición 3.20 (iii)).
(*c*) o v no satisface $\mathscr{B}$ o v satisface $\mathscr{C}$.
(*d*) o $v'(\mathscr{B}_0) = F$ o $v'(\mathscr{C}_0) = V$.
(*e*) $v'(\mathscr{B}_0 \rightarrow \mathscr{C}_0) = V$ (por Definición 2.12).
(*f*) $v'(\mathscr{A}_0) = V$.

Esto finaliza la demostración por inducción. La demostración de la proposición es ahora inmediata.

Sea $\mathscr{A}$ una *fbf* de $\mathscr{L}$ que es una tautología. Entonces $\mathscr{A}$ proviene por sustitución de una tautología $\mathscr{A}_0$ de L. Sea v una valoración de una interpretación I. Por lo recién demostrado, v satisface $\mathscr{A}$ si $v'(\mathscr{A}_0) = V$. Pero como $\mathscr{A}_0$ es tautología, v satisface $\mathscr{A}$. Así, $\mathscr{A}$ es verdadera en I.

▷ Hemos visto que en una interpretación dada no toda *fbf* es forzosamente verdadera o falsa. Consideremos, por ejemplo, la *fbf* $A_1^1(x_1)$ y una interpretación I para la cual D_I es $\mathbb{Z}$, el conjunto de los enteros, y la interpretación de A_1^1 es el predicado «>0». Entonces $A_1^1(x_1)$ se satisface para toda valoración v para la cual $v(x_1)>0$, pero no se satisface para ninguna valoración w tal que $w(x_1)\leqslant 0$. Intuitivamente, el si $A_1^1(x_1)$ se hace verdadera o no, depende de la interpretación de x_1. Esta situación surge muy frecuentemente al manejar una *fbf* en la que intervenga alguna variable libre. Nuestro siguiente resultado de importancia establece que una *fbf* en la que *no* aparecen variables libres es necesariamente verdadera o falsa en cualquier interpretación dada. Necesitamos algunos resultados auxiliares previos.

Definición 3.32

Una *fbf* $\mathscr{A}$ de $\mathscr{L}$ se llama *cerrada* si en $\mathscr{A}$ no aparecen variables libres.

Proposición 3.33

Sea I una interpretación para $\mathscr{L}$ y sea $\mathscr{A}$ una *fbf* de $\mathscr{L}$. Si v y w son valoraciones tales que $v(x_i)=w(x_i)$ para toda variable libre x_i de $\mathscr{A}$, entonces v satisface $\mathscr{A}$ si y sólo si w satisface $\mathscr{A}$.

Demostración: Por inducción sobre el número de conectivas y cuantificadores que intervienen en $\mathscr{A}$.

Paso base: $\mathscr{A}$ es una fórmula atómica, por ejemplo $A_i^n(t_1, \ldots, t_n)$ Las valoraciones v y w coinciden sobre las variables libres que aparecen en $t_1, \ldots, t_n$ y sobre todas las constantes individuales que aparecen, de modo que $v(t_i)=w(t_i)$ para $1\leqslant i\leqslant n$. Por lo tanto, v satisface $\mathscr{A}$ si y sólo si w satisface $\mathscr{A}$.

Paso de inducción:

Caso 1: $\mathscr{A}$ es $\sim\mathscr{B}$.
Caso 2: $\mathscr{A}$ es $(\mathscr{B}\rightarrow\mathscr{C})$.

Estos dos casos son inmediatos, sin más que utilizar las definiciones apropiadas. Se dejan como ejercicios.

Caso 3: $\mathscr{A}$ es $(\forall x_i)\mathscr{B}$.

Supongamos que v satisface $\mathscr{A}$, y sea w' i-equivalente a w. Entonces, como x_i no aparece libre en $(\forall x_i)\mathscr{B}$, tenemos $v(y)=w'(y)$ para toda variable y libre en $\mathscr{A}$. Ahora bien, cualquier v' que sea i-equivalente a v satisface $\mathscr{B}$; tomemos en particular la v' determinada por

$$v'(x_i)=w'(x_i)$$
$$v'(x_j)=v(x_j) \text{ si } j\neq i.$$

Entonces $w'(y) = v'(y)$ para toda variable y libre en $\mathscr{B}$. Así pues, por hipótesis de inducción y considerando que v' satisface $\mathscr{B}$, tenemos que w' satisface $\mathscr{B}$, con lo que w satisface $(\forall x_i)\mathscr{B}$.

La demostración de que si w satisface $(\forall x_i)\mathscr{B}$ entonces v satisface $(\forall x_i)\mathscr{B}$ procede del mismo modo.

Esto completa la inducción y demuestra el resultado.

Corolario 3.34

Si $\mathscr{A}$ es una *fbf* cerrada de $\mathscr{L}$ e I es una interpretación para $\mathscr{L}$, entonces $I \models \mathscr{A}$ o $I \models (\sim \mathscr{A})$.

Demostración: Sea $\mathscr{A}$ una *fbf* cerrada y sea I una interpretación. Sean v y w valoraciones arbitrarias. Trivialmente, $v(y) = w(y)$ siempre que y sea variable libre de $\mathscr{A}$ ($\mathscr{A}$ no tiene variables libres), de modo que v satisface $\mathscr{A}$ si y sólo si w satisface $\mathscr{A}$. Por lo tanto, o toda valoración satisface $\mathscr{A}$ o ninguna valoración satisface $\mathscr{A}$, es decir, o $\mathscr{A}$ es verdadera en I o $\mathscr{A}$ es falsa en I. Entonces, por la observación 3.25 (c), o $I \models \mathscr{A}$ o $I \models (\sim \mathscr{A})$.

▷ Este resultado es de interés para nosotros, ya que la noción de verdad en una interpretación es más importante que la de satisfacción con respecto a una valoración. Lo que hemos establecido es que para fórmulas *cerradas* todas las valoraciones en una cierta interpretación particular nos dan la misma respuesta en lo concerniente a la satisfacción de una fórmula dada. Así pues, para comprobar la verdad o falsedad de una *fbf* cerrada dada solamente necesitamos comprobar si alguna valoración la satisface o no. Veremos también que las fórmulas cerradas son de mayor importancia en lo que concierne a las propias matemáticas —de hecho, las fórmulas con variables libres a veces se comportan de una manera poco natural.

Las interpretaciones dan valores de verdad a las *fbfs* cerradas de $\mathscr{L}$. Puede suceder que para una *fbf* dada $\mathscr{A}$ de $\mathscr{L}$ todas las interpretaciones para $\mathscr{L}$ le den el valor V; es decir, que $\mathscr{A}$ sea verdadera en todas las posibles interpretaciones para $\mathscr{L}$.

Definición 3.35

Una *fbf* $\mathscr{A}$ de $\mathscr{L}$ es *lógicamente válida* si $\mathscr{A}$ es verdadera en toda interpretación para $\mathscr{L}$. $\mathscr{A}$ es *contradictoria* si $\mathscr{A}$ es falsa en toda interpretación.

Estas nociones son los análogos, dentro de la presente situación, de las nociones de tautología y contradicción del Capítulo 1. Del mismo modo que allí había fórmulas que no eran ni tautologías ni contradic-

ciones, en $\mathscr{L}$ hay fórmulas que no son ni lógicamente válidas ni contradictorias.

Observación 3.36

(*a*) Es consecuencia inmediata de la Proposición 3.26 que si las *fbfs* $\mathscr{A}$ y $(\mathscr{A}\rightarrow\mathscr{B})$ son lógicamente válidas, entonces $\mathscr{B}$ es lógicamente válida.

(*b*) De manera análoga, es consecuencia de la Proposición 3.27 que si la *fbf* $\mathscr{A}$ es lógicamente válida, también lo es $(\forall x_i)\mathscr{A}$, cualquiera que sea la variable x_i.

Ejemplo 3.37

(*a*) Hemos visto que toda *fbf* de $\mathscr{L}$ que provenga de una tautología de L por sustitución es lógicamente válida (Proposición 3.31). Nótese, pues, que la clase de las *fbfs* de $\mathscr{L}$ lógicamente válidas contiene a la clase de las tautologías.

(*b*) $((\forall x_i)\mathscr{A}\rightarrow(\exists x_i)\mathscr{A})$ es lógicamente válida, cualquiera que sea la *fbf* $\mathscr{A}$ de $\mathscr{L}$. Esto se demuestra por un método standard como sigue.

Sea I una interpretación de dominio D_I y sea v una valoración en I. Si v no satisface $(\forall x_i)\mathscr{A}$ entonces v satisface $((\forall x_i)\mathscr{A}\rightarrow(\exists x_i)\mathscr{A})$. Si v satisface $(\forall x_i)\mathscr{A}$, entonces toda valoración v' que sea i-equivalente a v satisface $\mathscr{A}$. Está claro, entonces, que existe una valoración i-equivalente a v que satisface $\mathscr{A}$. Así pues, v satisface $(\exists x_i)\mathscr{A}$, por la Proposición 3.29. Así pues, también en este caso v satisface $((\forall x_i)\mathscr{A}\rightarrow(\exists x_i)\mathscr{A})$. Hemos demostrado, pues, que una valoración arbitraria en una interpretación arbitraria satisface la *fbf* dada, con lo que ésta es lógicamente válida.

(*c*) $((\forall x_1)(\exists x_2)A_1^2(x_1, x_2)\rightarrow(\exists x_1)(\forall x_2)A_1^2(x_1, x_2))$ no es lógicamente válida. La demostración quizá es algo menos inmediata, puesto que lo que tenemos que hacer es encontrar una interpretación en la que la *fbf* dada no sea verdadera. Hemos de elegir un dominio D_I, una interpretación para la letra de predicado A_1^2, y una valoración que no satisfaga la *fbf*.

Sea $D_I=\mathbb{Z}$. Sea $A_1^2(y, z)$ la relación «$y<z$». Sin necesidad de escoger una valoración, está claro que la *fbf* cerrada $(\forall x_1)(\exists x_2)A_1^2(x_1, x_2)$ es verdadera en esta interpretación, y que $(\exists x_1)(\forall x_2)A_1^2(x_1, x_2)$ es falsa; es decir, toda valoración satisface la primera y no satisface la segunda. Así pues, ninguna valoración satisface la *fbf* dada. No es verdadera en esta interpretación, y no puede ser lógicamente válida.

(*d*) $A_1^1(x_1)$ no es lógicamente válida. Como vimos anteriormente (pág. 66), esta *fbf* no sólo no es lógicamente válida, sino que existen interpretaciones en las cuales no es ni verdadera ni falsa.

▷En general, para demostrar la validez lógica de una *fbf* dada, hemos de probar que una interpretación arbitraria la satisface. El demostrar que una *fbf* no es lógicamente válida generalmente requiere algo de ingenio para construir una interpretación concreta en la que haya una valoración que no la satisfaga.

Ejercicios

14 En la interpretación aritmética N del Ejemplo 3.5, encuéntrense, si es posible, valoraciones que satisfagan y que no satisfagan las siguientes *fbfs*.
- (*a*) $A_1^2(f_1^2(x_1, x_1), f_2^2(x_2, x_3))$.
- (*b*) $(A_1^2(f_1^2(x_1, a_1), x_2) \rightarrow A_1^2(f_1^2(x_1, x_2), x_3))$.
- (*c*) $\sim A_1^2(f_2^2(x_1, x_2), f_2^2(x_2, x_3))$.
- (*d*) $(\forall x_1) A_1^2(f_2^2(x_1, x_2), x_3)$.
- (*e*) $((\forall x_1) A_1^2(f_2^2(x_1, a_1), x_1) \rightarrow A_1^2(x_1, x_2))$.

15 En la interpretación descrita en el Ejercicio 11, encuéntrense, si es posible, valoraciones que satisfagan y que no satisfagan las siguientes *fbfs*.
- (*a*) $A_2^2(x_1, a_1)$.
- (*b*) $A_2^2(f_1^2(x_1, x_2), x_1) \rightarrow A_2^2(a_1, f_1^2(x_1, x_2))$.
- (*c*) $\sim A_2^2(x_1, f_1^2(x_1, x_2)))$.
- (*d*) $(\forall x_1) A_2^2(f_1^2(x_1, x_2), x_3)$.
- (*e*) $(\forall x_1) A_2^2(f_1^2(x_1, a_1) \rightarrow A_2^2(x_1, x_2)$.

16 ¿Cuáles de las siguientes *fbfs* son verdaderas en la interpretación N, y cuáles son falsas?
- (*a*) $(\forall x_1) A_1^2(f_2^2(x_1, a_1), x_1)$.
- (*b*) $(\forall x_1)(\forall x_2)(A_1^2(f_1^2(x_1, a_1), x_2) \rightarrow A_1^2(f_1^2(x_2, a_1), x_1))$.
- (*c*) $(\forall x_1)(\forall x_2)(\exists x_3) A_1^2(f_1^2(x_1, x_2), x_3)$.
- (*d*) $(\exists x_1) A_1^2(f_1^2(x_1, x_1), f_2^2(x_1, x_1))$.

17 ¿Cuáles de las siguientes *fbfs* cerradas son verdaderas en la interpretación del ejercicio 11, y cuáles son falsas?
- (*a*) $(\forall x_1) A_2^2(f_1^2(a_1, x_1), a_1)$.
- (*b*) $(\forall x_1)(\forall x_2)(\sim A_2^2(f_1^2(x_1, x_2), x_1))$.
- (*c*) $(\forall x_1)(\forall x_2)(\forall x_3)(A_2^2(x_1, x_2) \rightarrow A_2^2(f_1^2(x_1, x_3), f_1^2(x_2, x_3)))$.
- (*d*) $(\forall x_1)(\exists x_2) A_2^2(x_1, f_1^2(f_1^2(x_1, x_2), x_2))$.

18 Demuéstrese que, en una interpretación dada, la *fbf* $(\mathscr{A} \rightarrow \mathscr{B})$ es falsa si y sólo si $\mathscr{A}$ es verdadera y $\mathscr{B}$ es falsa. [Véase la Observación 3.25(*d*)].

19 Demuéstrese que cada una de las siguientes *fbfs* es lógicamente válida.
- (*a*) $((\exists x_1)(\forall x_2) A_1^2(x_1, x_2) \rightarrow (\forall x_2)(\exists x_1) A_1^2(x_1, x_2))$.
- (*b*) $(\forall x_1) A_1^1(x_1) \rightarrow ((\forall x_1) A_2^1(x_1) \rightarrow (\forall x_2) A_1^1(x_2))$.
- (*c*) $(\forall x_1)(\mathscr{A} \rightarrow \mathscr{B}) \rightarrow ((\forall x_1)\mathscr{A} \rightarrow (\forall x_1)\mathscr{B})$, para algunas *fbfs* $\mathscr{A}$ y $\mathscr{B}$.
- (*d*) $((\forall x_1)(\forall x_2)\mathscr{A} \rightarrow (\forall x_2)(\forall x_1)\mathscr{A})$, para algunas *fbf* $\mathscr{A}$.

20 Dése un ejemplo de *fbf* lógicamente válida que no sea cerrada.

21 Demuéstrese que si t es un término libre para x_i en la *fbf* $\mathscr{A}(x_i)$, entonces la *fbf* $(\mathscr{A}(t)\rightarrow(\exists x_i\ \mathscr{A}(x_i))$ es lógicamente válida.

22 Demuéstrese que ninguna de las siguientes *fbfs* es lógicamente válida.

(*a*) $(\forall x_1)(\exists x_2)A_1^2(x_1,\ x_2)\rightarrow(\exists x_2)(\forall x_1)A_1^2(x_1,\ x_2)$.
(*b*) $(\forall x_1)(\forall x_2)(A_1^2(x_1,\ x_2)\rightarrow A_1^2(x_2,\ x_1))$.
(*c*) $(\forall x_1)(\sim A_1^1(x_1))\rightarrow(\sim A_1^1(a_1)))$.
(*d*) $((\forall x_1)A_1^2(x_1,\ x_1)\rightarrow(\exists x_2)(\forall x_1)A_1^2(x_1,\ x_2))$.

23 Sea $\mathscr{A}(x_i)$ una *fbf* de $\mathscr{L}$ en la que x_i aparece libre y sea t un término libre para x_i en $\mathscr{A}(x_i)$. Supongamos que v es una valoración tal que $v(t)=v(x_i)$. Demuéstrese que v satisface $\mathscr{A}(t)$ si y sólo si v satisface $\mathscr{A}(x_i)$.

4
Cálculo de Predicados Formal

4.1 El sistema formal $K_{\mathscr{L}}$

En el Capítulo 3 hemos descrito los lenguajes formales que vamos a utilizar, y hemos visto cómo diferentes tipos de enunciados pueden trasladarse a *fbfs* de lenguajes de primer orden apropiados. Los mismo que hicimos en el Capítulo 3, consideramos en este capítulo un lenguaje de primer orden fijo y no especificado $\mathscr{L}$, con el fin de que nuestros resultados sean generales y se apliquen a todos los lenguajes de primer orden. Los símbolos de $\mathscr{L}$ pueden interpretarse de muchos modos diferentes, pero ahora nos ocuparemos de los aspectos puramente formales del lenguaje y consideraremos relaciones lógicas entre *fbfs* más bien que propiedades que dependan de interpretaciones particulares. El esquema a seguir es similar al del Capítulo 2: Definiremos un sistema deductivo formal y demostraremos seguidamente que tiene las propiedades que debe tener: Es decir, que es consistente y que la clase de sus teoremas es precisamente la clase de las *fbfs* lógicamente válidas.

Fijemos un lenguaje de primer orden $\mathscr{L}$. Definamos un sistema deductivo formal $K_{\mathscr{L}}$ por medio de los siguientes axiomas y reglas de deducción.

Axiomas

Sean $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ *fbfs* cualesquiera de $\mathscr{L}$. Las siguientes *fbfs* son axiomas de $K_{\mathscr{L}}$:

($K1$) $(\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$.

($K2$) $(\mathscr{A}\rightarrow(\mathscr{B}\rightarrow\mathscr{C}))\rightarrow((\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\mathscr{A}\rightarrow\mathscr{C}))$.

($K3$) $(\sim\mathscr{A}\rightarrow\sim\mathscr{B})\rightarrow(\mathscr{B}\rightarrow\mathscr{A})$.

($K4$) $((\forall x_i)\,\mathscr{A}\rightarrow\mathscr{A})$, si x_i no aparece libre en $\mathscr{A}$.

($K5$) $((\forall x_i)\rightarrow\mathscr{A}(t))$, si $\mathscr{A}(x_i)$ es una *fbf* de $\mathscr{L}$ y t es un término de $\mathscr{L}$ libre para x_i en $\mathscr{A}(x_i)$.

($K6$) $(\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\mathscr{A}\rightarrow(\forall x_i)\,\mathscr{B})$, si $\mathscr{A}$ no tiene intervenciones libres de la variable x_i.

Nótese que éstos son esquemas de axioma, cada uno con infinitas realizaciones posibles.

Reglas

(1) *Modus ponens*, es decir, de $\mathscr{A}$ y $(\mathscr{A} \rightarrow \mathscr{B})$ se deduce $\mathscr{B}$, siendo $\mathscr{A}$ y $\mathscr{B}$ *fbfs* cualesquiera de $\mathscr{L}$.

(2) Generalización, es decir, de $\mathscr{A}$ se deduce $(\forall x_i)\mathscr{A}$, siendo $\mathscr{A}$ cualquier *fbf* de $\mathscr{L}$ y x_i cualquier variable.

Observación 4.1

(*a*) Los esquemas de axioma y las reglas de deducción para $K_{\mathscr{L}}$ incluyen los esquemas de axiomas y la regla de *L*. Los axiomas y la regla adicionales se necesitan para las demostraciones en las que intervienen propiedades de los cuantificadores.

(*b*) El axioma (*K*5) se ha enunciado en su forma más general. En las aplicaciones nos encontramos frecuentemente con el caso particular $((\forall x_i)\mathscr{A} \rightarrow \mathscr{A})$, donde x_i puede o no aparecer libre en $\mathscr{A}$. Si x_i aparece libre en $\mathscr{A}$ podemos escribir $\mathscr{A}$ como $\mathscr{A}(x_i)$, y (*K*5) nos proporciona $((\forall x_i) \rightarrow \mathscr{A}(x_i))$, ya que x_i está libre para x_i en $\mathscr{A}(x_i)$. Si x_i no aparece libre en $\mathscr{A}$, entonces (*K*4) nos da $((\forall x_i)\mathscr{A} \rightarrow \mathscr{A})$.

Definición 4.2

(Véase Definición 2.2). Una *demostración* en $K_{\mathscr{L}}$ es una sucesión finita $\mathscr{A}_1, \ldots, \mathscr{A}_n$ de *fbfs*. de $\mathscr{L}$ tal que para todo $i (1 \leqslant i \leqslant n)$, o $\mathscr{A}_i$ es axioma de $K_{\mathscr{L}}$ o $\mathscr{A}_i$ se deduce de miembros anteriores de la sucesión por *MP* o generalización.

Si Γ es un conjunto de *fbfs* de $\mathscr{L}$, una *deducción a partir de* Γ en $K_{\mathscr{L}}$ es una sucesión similar, en la que pueden incluirse además elementos de Γ. (Véase Definición 2.5.)

Una *fbf* $\mathscr{A}$ es un *teorema* de $K_{\mathscr{L}}$ si es el último miembro de una sucesión finita que constituye una demostración en $K_{\mathscr{L}}$.

Una *fbf* $\mathscr{A}$ es *consecuencia* en $K_{\mathscr{L}}$ del conjunto de *fbfs*. Γ si $\mathscr{A}$ es el último miembro de una sucesión finita que constituya una deducción a partir de Γ en $K_{\mathscr{L}}$.

Escribiremos $\underset{K_{\mathscr{L}}}{\vdash} \mathscr{A}$ para denotar «$\mathscr{A}$ es un teorema de $K_{\mathscr{L}}$», y $\Gamma \underset{K_{\mathscr{L}}}{\vdash} \mathscr{A}$ para denotar «$\mathscr{A}$ es una consecuencia de Γ en $K_{\mathscr{L}}$», siendo Γ un conjunto de *fbfs* de $K_{\mathscr{L}}$.

Por conveniencia, abreviaremos $K_{\mathscr{L}}$ a *K*, salvo que haya alguna razón para hacer énfasis en el lenguaje particular utilizado.

Proposición 4.3

Si $\mathscr{A}$ es una *fbf* de $\mathscr{L}$ y $\mathscr{A}$ es una tautología, entonces $\mathscr{A}$ es un teorema de K. (Veremos que la recíproca es falsa, en contraste con la situación del Capítulo 2.)

Demostración: Una *fbf* $\mathscr{A}$ de $\mathscr{L}$ es una tautología si existe una *fbf* $\mathscr{A}_0$ de $\mathscr{L}$ a partir de la cual puede obtenerse $\mathscr{A}$ sustituyendo *fbfs* de $\mathscr{L}$ en lugar de las variables de enunciado, y que es una tautología. Sea $\mathscr{A}$ una *fbf* de $\mathscr{L}$ que es tautología, y sea $\mathscr{A}_0$ la correspondiente *fbf* de L. Entonces $\mathscr{A}_0$ es una tautología, luego $\vdash_L \mathscr{A}_0$. La demostración de $\mathscr{A}_0$ en L puede transformarse en una demostración de $\mathscr{A}$ en K, sin más que reemplazar variables de enunciado por *fbfs* de $\mathscr{L}$ apropiadas en todas sus intervenciones. Lo que se obtiene es una demostración en K, ya que los esquemas de axioma ($L1$), ($L2$), ($L3$) y la regla MO son comunes a los sistemas L y K. Así tenemos que $\vdash_K \mathscr{A}$, como se quería.

▷ Hay una proposición análoga a la Proposición 2.14 vista para el sistema L. Afirma que todo teorema de K es lógicamente válido. La demostración sigue un curso parecido a la de 2.14; hemos de empezar comprobando que los axiomas de K son todos lógicamente válidos. Ya hemos demostrado que todos los casos particulares de ($K1$), ($K2$) y ($K3$) son lógicamente válidos (Proposición 3.29), puesto que son tautologías.

Proposición 4.4

Todos los casos particulares de los esquemas de axioma ($K4$), ($K5$) y ($K6$) son lógicamente válidos.

Demostración: Para ($K4$), tomemos una valoración v en una interpretación I para $\mathscr{L}$, y supongamos que v satisface $(\forall x_i)\mathscr{A}$. Entonces cualquier v' que sea i-equivalente a v satisface $\mathscr{A}$. En particular, v satisface $\mathscr{A}$. Así pues, toda valoración en I satisface $((\forall x_i)\mathscr{A} \rightarrow \mathscr{A})$, con lo que $I \models ((\forall x_i)\mathscr{A} \rightarrow \mathscr{A})$ para toda interpretación I, es decir, $((\forall x_i)\mathscr{A} \rightarrow \mathscr{A})$ es lógicamente válida.

Para ($K5$), supongamos que t está libre para x_i en la *fbf* $\mathscr{A}(x_i)$, y sea v una valoración en una interpretación I. Si v no satisface $(\forall x_i)\mathscr{A}(x_i)$, entonces v satisface $((\forall x_i)\mathscr{A}(x_i) \rightarrow \mathscr{A}(t))$ (Definición 3.20). Supongamos pues que v satisface $(\forall x_i)\mathscr{A}(x_i)$. Demostraremos que v satisface también $\mathscr{A}(t)$. Toda w que sea i-equivalente a v satisface $\mathscr{A}(x_i)$. En particular, v' satisface $\mathscr{A}(x_i)$, siendo $v'(x_i) = v(t)$ y $v'(x_k) = v(x_k)$ para $k \neq i$. Así pues, por la Proposición 3.23, v satisface $\mathscr{A}(t)$. Se deduce ahora que toda valoración v en I satisface $((\forall x_i)\mathscr{A}(x_i) \rightarrow \mathscr{A}(t))$, con lo que $I \models ((\forall x_i)\mathscr{A}(x_i) \rightarrow \mathscr{A}(t))$ para toda I, es decir, $((\forall x_i)\mathscr{A}(x_i) \rightarrow \mathscr{A}(t))$ es lógicamente válida, como se quería.

Para ($K6$), sean $\mathscr{A}$ y $\mathscr{B}$ *fbfs.* de $\mathscr{L}$ y supongamos que x_i no aparece libre en $\mathscr{A}$. Sea v una valoración en una interpretación I. La verificación sigue el mismo esquema anterior. Supongamos que v satisface $(\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})$. Entonces toda w que sea i-equivalente a v satisface $(\mathscr{A}\rightarrow\mathscr{B})$. Así pues, cada una de estas w satisface a $\mathscr{B}$ o no satisface a $\mathscr{A}$. Ahora, si una de estas w no satisface a $\mathscr{A}$, ninguna de ellas satisface a $\mathscr{A}$, pues x_i no aparece libre en $\mathscr{A}$ (por la Proposición 3.3). v es una de las w, así que tenemos:

o bien v no satisface $\mathscr{A}$,
o toda w que sea i-equivalente a v satisface $\mathscr{B}$.

Así pues,

o v no satisface $\mathscr{A}$ o v satisface $(\forall x_i)\mathscr{B}$.

Es decir, v satisface $(\mathscr{A}\rightarrow(\forall x_i)\mathscr{B})$. Por tanto, toda valoración en I satisface $(\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\mathscr{A}\rightarrow(\forall x_i)\mathscr{B})$. Se deduce entonces, al igual que antes, que $(\forall x_i)((\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\mathscr{A}\rightarrow(\forall x_i)\mathscr{B})$ es lógicamente válida.

Proposición 4.5 (El teorema de Corrección para K)

Para toda *fbf* $\mathscr{A}$ de $\mathscr{L}$, si $\vdash_K \mathscr{A}$ entonces $\mathscr{A}$ es lógicamente válida.

Demostración: Por inducción sobre el número de pasos de una demostración de $\mathscr{A}$.

Paso base: Si $\mathscr{A}$ posee una demostración de un solo paso, entonces $\mathscr{A}$ es un axioma de K. Más arriba hemos demostrado que todo axioma de K es lógicamente válido.

Paso de inducción: Supongamos que $\mathscr{A}$ posee una demostración con n pasos ($n>1$) y que todos los teoremas de K que tienen demostraciones de menos de n pasos son lógicamente válidos. $\mathscr{A}$ aparece en una demostración, así que o $\mathscr{A}$ es un axioma, o $\mathscr{A}$ se deduce de *fbfs* anteriores de la demostración usando *MO* o Generalización. Si $\mathscr{A}$ es un axioma, entonces $\mathscr{A}$ es lógicamente válida, lo mismo que antes. Si $\mathscr{A}$ se deduce de $\mathscr{B}$ y $(\mathscr{B}\rightarrow\mathscr{A})$, *fbfs* anteriores de la demostración, por medio de *MP*, entonces $\mathscr{B}$ y $(\mathscr{B}\rightarrow\mathscr{A})$ poseen demostraciones de longitud menor y son por tanto lógicamente válidas, por hipótesis de inducción. Por la Observación 3.36(a), $\mathscr{A}$ es entonces lógicamente válida. Así mismo, si $\mathscr{A}$ se deduce mediante Generalización de una *fbf* anterior, digamos $\mathscr{C}$, entonces $\mathscr{C}$ es lógicamente válida, y $\mathscr{A}$, que es $(\forall x_i)\,\mathscr{C}$, es también lógicamente válida, por la Observación 3.36(a). Así pues, en todos los casos $\mathscr{A}$ es lógicamente válida.

Esto completa la demostración por inducción.

Corolario 4.6

K es consistente (es decir, para ninguna *fbf* $\mathscr{A}$ se cumple que $\mathscr{A}$ y $\sim\mathscr{A}$ son teoremas de K).

Demostración: Supongamos que $\vdash_K \mathscr{A}$ y $\vdash_K (\sim\mathscr{A})$ para alguna *fbf* $\mathscr{A}$ de $\mathscr{L}$. Entonces $\mathscr{A}$ y $(\sim\mathscr{A})$ son ambas lógicamente válidas, por la Proposición 4.5. Por lo tanto, en toda interpretación $\mathscr{A}$ y $(\sim\mathscr{A})$ son ambas verdaderas.

Esto contradice la Observación 3.25(*c*), luego K debe ser consistente.

▷ El encontrar demostraciones en K para teoremas de K es difícil, como lo era para L, y de nuevo buscamos métodos que nos ayuden a demostrar que ciertas *fbfs* particulares son teoremas. En K existe una proposición que corresponde al Teorema de Deducción (Proposición 2.8), pero que es algo más complicada. Veamos en un ejemplo de qué va a tratarse.

Ejemplo 4.7

Sabemos que para toda *fbf* $\mathscr{A}$ de K, $\mathscr{A} \vdash_K (\forall x_1)\,\mathscr{A}$ (esto es inmediato, por la regla de Generalización). No obstante, no es cierto necesariamente que $\vdash_K (\mathscr{A} \to (\forall x_1)\,\mathscr{A})$.

Para ver esto, tomemos $A_1^1(x_1)$ como $\mathscr{A}$. Sea I una interpretación cuyo dominio sea el conjunto Z de los enteros, y sea $\overline{A}_1^1$ el predicado «$=0$». $A_1^1(x_1)$ se interpreta entonces intuitivamente como «$x=0$». Toda valoración en I para la cual $v(x_1)=0$ satisfacerá $A_1^1(x_1)$. No obstante, cualquier valoración 1-equivalente a esta v (y diferente de ella) no satisfacerá $A_1^1(x_1)$. Por lo tanto, ninguna valoración en I satisface $(\forall x_1)\,A_1^1(x_1)$. Existe pues una valoración que satisface $A_1^1(x_1)$ pero que no satisface $(\forall x_1)\,A_1^1(x_1)$. Esta valoración no satisface $(A_1^1(x_1) \to (\forall x_1)\,A_1^1(x_1))$, por lo cual esta *fbf* no es verdadera en I. Así pues, no es lógicamente válida, con lo cual, por la Proposición 4.5, no puede ser un teorema de K.

Proposición 4.8 (El teorema de Deducción para K)

Sean $\mathscr{A}$ y $\mathscr{B}$ *fbfs* de $\mathscr{L}$ y sea Γ un conjunto (eventualmente vacío) de *fbfs* de $\mathscr{L}$. Si $\Gamma \cup \{A\} \vdash_K \mathscr{B}$, y si la deducción no contiene aplicaciones de la regla de Generalización con respecto a una variable que aparezca libre en $\mathscr{A}$, entonces $\Gamma \vdash_K (\mathscr{A} \to \mathscr{B})$.

Demostración: La demostración es por inducción sobre n, el número de *fbfs* de la deducción de $\mathscr{B}$ a partir de $\Gamma \cup \{A\}$.

Paso base: $n=1$. $\mathscr{B}$ es un axioma, o $\mathscr{A}$, o un miembro de Γ. Deducimos que $\Gamma \vdash_K (\mathscr{A} \to \mathscr{B})$ del mismo modo que en la correspondiente demostración del Teorema de Deducción para L.

Paso de inducción: Sea $n>1$. Supongamos que si $\mathscr{F}$ es una *fbf* de $\mathscr{L}$ que puede deducirse a partir de $\Gamma \cup \{\mathscr{A}\}$ sin aplicar la regla de Ge-

neralización a una variable libre de $\mathscr{A}$, y en una deducción con menos de n *fbfs*, entonces $\Gamma \vdash_K (\mathscr{A} \to \mathscr{F})$.

Caso 1: $\mathscr{B}$ se deduce de *fbfs* anteriores de la deducción, por medio de *MP*. La demostración es en este caso la misma que para *L*.

Caso 2: $\mathscr{B}$ es un axioma, o $\mathscr{A}$, o un miembro de Γ. La demostración es, de nuevo, como para *L*.

Caso 3: $\mathscr{B}$ se deduce de una *fbf* anterior de la deducción, mediante generalización. Así, $\mathscr{B}$ es $(\forall x_i)\,\mathscr{C}$, pongamos por caso, y $\mathscr{C}$ aparece en un lugar anterior de la deducción. Por tanto, $\Gamma \cup \{A\} \vdash_K \mathscr{C}$, con la deducción de menos de n *fbfs* de modo que $\Gamma \vdash_K (\mathscr{A} \to \mathscr{C})$, ya que no hay ninguna aplicación de la regla de Generalización referida a una variable libre de $\mathscr{A}$. Tampoco x_i puede aparecer libre en $\mathscr{A}$, ya que a ella se refiere una aplicación de la regla de Generalización en la deducción de $\mathscr{B}$ a partir de $\Gamma \cup \{\mathscr{A}\}$. Así pues, obtenemos una deducción de $(\mathscr{A} \to \mathscr{B})$ a partir de Γ como sigue:

(1)		deducción de $(\mathscr{A} \to \mathscr{C})$ a partir de Γ
⋮		
⋮		
(k)	$(\mathscr{A} \to \mathscr{C})$	
$(k+1)$	$(\forall x_i)(\mathscr{A} \to \mathscr{C})$	(k), Generalización
$(k+2)$	$(\forall x_i)(\mathscr{A} \to \mathscr{C}) \to (\mathscr{A} \to (\forall x_i)\mathscr{C})$	$(K6)$
$(k+3)$	$(\mathscr{A} \to (\forall x_i)\mathscr{C})$	$(k+1)$, $(k+2)$, *MP*.

Así, $\Gamma \vdash_K (\mathscr{A} \to \mathscr{B})$ como se quería, lo que concluye nuestra demostración inductiva.

▷ Esta es la versión más útil del Teorema de Deducción para *K*. Es posible debilitar la condición adicional referente al uso de la Generalización (véase pág. 61 de Mendelson), pero nosotros no vamos a tener necesidad de hacerlo. Fortaleciendo esta condición adicional resulta el siguiente corolario, que es útil a menudo.

Corolario 4.9

Si $\Gamma \cup \{A\} \vdash_K \mathscr{B}$ y $\mathscr{A}$ es una *fbf* cerrada, entonces $\Gamma \vdash_K (\mathscr{A} \to \mathscr{B})$.

Pese a la forma aparentemente menos general del Teorema de Deducción para *K*, podemos continuar aplicándolo con éxito para demostrar que ciertas *fbfs* son teoremas, al igual que hicimos para *L*.

Corolario 4.10

Dadas *fbfs* cualesquiera $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ de $\mathscr{L}$,

$$\{(\mathscr{A} \to \mathscr{B}), (\mathscr{B} \to \mathscr{C})\} \vdash_K (\mathscr{A} \to \mathscr{C})$$

Demostración: Idéntica a la del Corolario 2.10.

▷Nótese pues que la regla SH puede usarse legítimamente en K, lo mismo que en L. Al Al igual que en L, el Teorema de Deducción para K tiene un recíproco.

Proposición 4.11

Supongamos que $\mathscr{A}$ y $\mathscr{B}$ son *fbfs* de $\mathscr{L}$, que Γ es un conjunto de *fbfs* de $\mathscr{L}$, y que $\Gamma \vdash_K (\mathscr{A} \to \mathscr{B})$. Entonces $\Gamma \cup \{\mathscr{A}\} \vdash_K \mathscr{B}$.

Demostración: Idéntica a la demostración de la Proposición 2.9.

Ejemplo 4.12

Si x_i no aparece libre en $\mathscr{A}$, entonces

$$\vdash_K ((\mathscr{A} \to (\forall x_i)\mathscr{B}) \to (\forall x_i)(\mathscr{A} \to \mathscr{B})).$$

Escribamos una deducción.

(1)	$(\mathscr{A} \to (\forall x_i)\,\mathscr{B})$	hipótesis
(2)	$(\forall x_i)\,\mathscr{B} \to \mathscr{B}$	($K4$) o ($K5$)
(3)	$(\mathscr{A} \to \mathscr{B})$	(1), (2), SH
(4)	$(\forall x_i)(\mathscr{A} \to \mathscr{B})$	(3), Generalización

Por lo tanto, tenemos:

$$(\mathscr{A} \to (\forall x_i)\mathscr{B}) \vdash_K (\forall x_i)(\mathscr{A} \to \mathscr{B})$$

Ahora bien, la regla de Generalización se ha usado en la deducción, pero afectando solamente a la variable x_i, que no aparece libre en $(\mathscr{A} \to (\forall x_i)\mathscr{B})$. Así pues, podemos aplicar el Teorema de Deducción, obteniendo:

$$\vdash_K ((\mathscr{A} \to (\forall x_i)\mathscr{B}) \to (\forall x_i)(\mathscr{A} \to \mathscr{B})),$$

como se quería.

Ejemplo 4.13

Para *fbfs* cualesquiera $\mathscr{A}$, $\mathscr{B}$ de $\mathscr{L}$

$$\vdash_K ((\forall x_i)\ (\mathscr{A} \to \mathscr{B}) \to ((\exists x_i)\,\mathscr{A} \to (\exists x_i)\mathscr{B})).$$

Escribamos una deducción. El paso (2) no parece obvio a primera vista, pero al final veremos la razón por la que se incluye.

(1)	$(\forall x_i)\ (\mathscr{A} \to \mathscr{B})$	hipótesis
(2)	$(\forall x_i)\ (\sim \mathscr{B})$	hipótesis
(3)	$(\forall x_i)\ (\mathscr{A} \to \mathscr{B}) \to (\mathscr{A} \to \mathscr{B})$	($K4$) o ($K5$)

(4)	$(\mathscr{A}\rightarrow\mathscr{B})$	(1), (3), MP
(5)	$(\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\sim\mathscr{B}\rightarrow\sim\mathscr{A})$	tautología
(6)	$(\sim\mathscr{B}\rightarrow\sim\mathscr{A})$	(4), (5), MP
(7)	$((\forall x_i)\ (\sim\mathscr{B})\rightarrow(\sim\mathscr{B}))$	($K4$), o ($K5$)
(8)	$(\sim\mathscr{B})$	(2), (7), MP
(9)	$(\sim\mathscr{A})$	(6), (8), MP
(10)	$(\forall x_i)\ (\sim\mathscr{A})$	(9), Generalización

Esto demuestra que

$$\{(\forall x_i)(\mathscr{A}\rightarrow\mathscr{B}),\ (\forall x_i)(\sim\mathscr{B})\}\ \vdash_{\overline{K}}\ (\forall x_i)(\sim\mathscr{A})$$

Por el Teorema de Deducción, obtenemos

$$(\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})\ \vdash_{\overline{K}}\ ((\forall x_i)(\sim\mathscr{B})\rightarrow(\forall x_i)(\sim\mathscr{A}))$$

ya que x_i no aparece libre en $(\forall x_i)(\sim\mathscr{B})$. Ahora bien, sabemos que

$$\vdash_{\overline{K}}\ ((\forall x_i)(\sim\mathscr{B})\rightarrow(\forall x_i)(\sim\mathscr{A}))\rightarrow(\sim(\forall x_i)(\sim\mathscr{A})\rightarrow\sim(\forall x_i)(\sim\mathscr{B}))$$

por lo que, usando MP, se tiene

$$(\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})\ \vdash_{\overline{K}}\ (\sim(\forall x_i)(\sim\mathscr{A})\rightarrow\sim(\forall x_i)(\sim\mathscr{B}))$$

es decir,

$$(\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})\ \vdash_{\overline{K}}\ ((\exists x_i)\,\mathscr{A}\rightarrow(\exists x_i)\mathscr{B}).$$

Usando de nuevo el Teorema de Deducción,

$$\vdash_{\overline{K}}((\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})\rightarrow((\exists x_i)\mathscr{A}\rightarrow(\exists x_i)\mathscr{B})),$$

puesto que x_i no aparece libre en $(\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})$.

Ejercicios

1 Escríbase una demostración en $K_{\mathscr{L}}$ de la *fbf*

$$(\forall x_1)(A_1^1(x_1)\rightarrow A_1^1(x_1)).$$

2 Demuéstrese que son teoremas de $K_{\mathscr{L}}$

(*a*) $(\exists x_i)(\mathscr{A}\rightarrow\mathscr{B})\rightarrow((\forall x_i)\mathscr{A}\rightarrow\mathscr{B})$,

(*b*) $((\exists x_i)\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})$, supuesto que x_i no aparezca libre en $\mathscr{B}$.

(*c*) $\vdash(\sim(\forall x_i)\mathscr{A}\rightarrow(\exists x_i)\sim\mathscr{A})$.

3 (*a*) ¿Dónde está el error en lo que sigue?

(1)	$(\exists x_2)A_2^1(x_1, x_2)$	hipótesis
(2)	$(\forall x_1)(\exists x_2)A_2^1(x_1, x_2)$	(1), Generalización
(3)	$(\forall x_1)(\exists x_2)A_1^2(x_1, x_2)\rightarrow(\exists x_2)A_1^2(x_2, x_2)$	$K5$
(4)	$(\exists x_2)A_1^2(x_2, x_2)$	(2), (3), MP

Así pues, $(\exists x_2)A_1^2(x_1, x_2)\ \vdash_{\overline{K}}\ (\exists x_2)A_1^2(x_2, x_2)$, con lo cual, por el Teorema de Deducción,

$$\vdash_K (\exists x_2) A_1^2(x_1, x_2) \rightarrow (\exists x_2) A_1^2(x_2, x_2)$$

(*b*) Demuéstrese, encontrando una interpretación adecuada, que la fórmula $((\exists x_2) A_1^2(x_1, x_2) \rightarrow (\exists x_2) A_1^2(x_2, x_2))$ no es lógicamente válida, por lo que no es un teorema de *K*.

4.2 Equivalencia, sustitución

Observación 4.14

Es conveniente introducir la conectiva $\leftrightarrow$ como símbolo definido de nuestro lenguaje. Dadas *fbfs* $\mathscr{A}$ y $\mathscr{B}$ de $\mathscr{L}$, $(\mathscr{A} \leftrightarrow \mathscr{B})$ representa $\sim((\mathscr{A} \rightarrow \mathscr{B}) \rightarrow \sim(\mathscr{B} \rightarrow \mathscr{A}))$. Nótese que $(\mathscr{B} \leftrightarrow \mathscr{A})$ no es una *fbfs* de $\mathscr{L}$, sino que la usamos como abreviatura conveniente de una cierta *fbf*.

Proposición 4.15

Para *fbfs* cualesquiera $\mathscr{A}$ y $\mathscr{B}$ de $\mathscr{L}$, $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{B})$ si y sólo si $\vdash_K (\mathscr{A} \rightarrow \mathscr{B})$ y $\vdash_K (\mathscr{B} \rightarrow \mathscr{A})$.

Demostración: Supongamos primeramente que $\vdash_K (\mathscr{A} \rightarrow \mathscr{B})$, es decir, $\vdash_K \sim((\mathscr{A} \rightarrow \mathscr{B}) \rightarrow \sim(\mathscr{B} \rightarrow \mathscr{A}))$.
Las *fbfs* $(\sim((\mathscr{A} \rightarrow \mathscr{B}) \rightarrow \sim(\mathscr{B} \rightarrow \mathscr{A})) \rightarrow (\mathscr{A} \rightarrow \mathscr{B}))$ y

$$(\sim((\mathscr{A} \rightarrow \mathscr{B}) \rightarrow \sim(\mathscr{B} \rightarrow \mathscr{B}) \rightarrow (\mathscr{B} \rightarrow \mathscr{A}))$$

son tautologías (se deja la comprobación al lector), por lo cual, por la Proposición 4.3, son teoremas de *K*. Por *MP*, entonces, tenemos

$$\vdash_K (\mathscr{A} \rightarrow \mathscr{B}) \text{ y } \vdash_K (\mathscr{B} \rightarrow \mathscr{A})$$

como se quería.

Supongamos ahora que $\vdash_K (\mathscr{A} \rightarrow \mathscr{B})$ y $\vdash_K (\mathscr{B} \rightarrow \mathscr{A})$. Hemos de demostrar que $\vdash_K \sim((\mathscr{A} \rightarrow \mathscr{B}) \rightarrow \sim(\mathscr{B} \rightarrow \mathscr{A}))$. Es suficiente demostrar que la *fbf*

$$(\mathscr{A} \rightarrow \mathscr{B}) \rightarrow ((\mathscr{B} \rightarrow \mathscr{A}) \rightarrow \sim((\mathscr{A} \rightarrow \mathscr{B}) \rightarrow \sim(\mathscr{B} \rightarrow \mathscr{A})))$$

es una tautología, y esto puede hacerse fácilmente construyendo una tabla de verdad.

Definición 4.16

Si $\mathscr{A}$ y $\mathscr{B}$ son *fbfs* de $\mathscr{L}$ y $\vdash_K (\mathscr{A} \leftrightarrow \mathscr{B})$, diremos que *la equivalencia entre* $\mathscr{A}$ *y* $\mathscr{B}$ *es demostrable.*

Corolario 4.17

Para *fbfs* cualesquiera $\mathscr{A}$, $\mathscr{B}$, $\mathscr{C}$ de $\mathscr{L}$, si es demostrable la equivalencia de $\mathscr{A}$ y $\mathscr{B}$ y es demostrable la equivalencia de $\mathscr{B}$ y $\mathscr{C}$, entonces es demostrable la equivalencia de $\mathscr{A}$ y $\mathscr{C}$.

Demostración: Sea $\vdash_K(\mathscr{A}\leftrightarrow\mathscr{B})$ y $\vdash_K(\mathscr{B}\leftrightarrow\mathscr{C})$. Entonces $\vdash_K(\mathscr{A}\rightarrow\mathscr{B})$ y $\vdash_K(\mathscr{B}\rightarrow\mathscr{C})$, de modo que por SH tenemos $\vdash_K(\mathscr{A}\rightarrow\mathscr{B})$.

Asimismo, $\vdash_K(\mathscr{B}\rightarrow\mathscr{A})$ y $\vdash_K(\mathscr{C}\rightarrow\mathscr{B})$, y de nuevo por *SH* se tiene $\vdash_K(\mathscr{C}\rightarrow\mathscr{A})$. Así pues, por la Proposición 4.15, $\vdash_K(\mathscr{A}\leftrightarrow\mathscr{C})$.

▷ Esta última proposición será útil cuando necesitemos demostrar que la equivalencia de dos *fbfs* es demostrable. Necesitaremos hacerlo en la siguiente parte de nuestra descripción de K, en la que investigaremos cómo pueden hacerse sustituciones en el lugar de partes de *fbfs* y en el lugar de variables. Esto lo hicimos de manera informal en el Capítulo 1. Aquí, la presencia de variables complica las cosas, por lo que algunas de las demostraciones son tediosas. No obstante, los resultados se usarán posteriormente, así que esta parte de nuestra exposición es necesaria.

Comencemos considerando el modo en que pueden efectuarse sustituciones en el lugar de variables. La *fbf* $(\forall x_1)A_1^1(x_1)$ se interpretará (intuitivamente) como 'para todo x, se verifica $A_1^1(x)$'. Del mismo modo, la *fbf* $(\forall x_2)A_1^1(x_2)$ se interpretará como 'para todo x, se verifica $A_1^1(x)$'. Parece pues que la variable que de hecho aparezca en la *fbf* no afecta (en este caso) a la interpretación. Por consiguiente, en el sistema formal K estas dos *fbfs.* deberán ser equivalentes en algún sentido. Esto se precisa en la siguiente proposición.

Como antes, supongamos que $\mathscr{A}(x_i)$ denota una *fbf* de $\mathscr{L}$ en la que aparece libre x_i (eventualmente más de una vez). Entonces, para cualquier variable x_j, denotaremos por $\mathscr{A}(x_j)$ la *fbf* obtenida sustituyendo x_j en el lugar de cada intervención libre de x_i en $\mathscr{A}(x_i)$.

Proposición 4.18

Si x_i aparece libre en $\mathscr{A}(x_i)$ y x_j es una variable que no aparece ni libre ni ligada en $\mathscr{A}(x_i)$, entonces

$$\vdash_K((\forall x_i)\,\mathscr{A}(x_i)\leftrightarrow(\forall x_j)\,\mathscr{A}(x_j))$$

Demostración: Obsérvese primero que, bajo las condiciones especificadas, x_i está libre para x_j en $\mathscr{A}(x_j)$ y x_j está libre para x_i en $\mathscr{A}(x_i)$. Necesitamos dos deducciones, para demostrar que ambas implicaciones son teoremas de K.

(1)	$(\forall x_i)\,\mathscr{A}(x_i)$	hipótesis
(2)	$((\forall x_i)\,\mathscr{A}(x_i)\rightarrow\mathscr{A}(x_i))$	$(K5)$
(3)	$\mathscr{A}(x_j)$	(1), (2), MP
(4)	$(\forall x_j)\,\mathscr{A}(x_j)$	(3), Generalización
$\therefore$	$(\forall x_i)\,\mathscr{A}(x_i)\vdash_K(\forall x_j)\,\mathscr{A}(x_j)$	

Así pues, por el Teorema de Deducción,

$$\vdash_K((\forall x_i)\,\mathscr{A}(x_i)\rightarrow(\forall x_j)\,\mathscr{A}(x_j))$$

puesto que x_j no está libre en $(\forall x_i)\,\mathscr{A}(x_i)$. Del mismo modo demostraremos que

$$\vdash_K((\forall x_j)\,\mathscr{A}(x_j)\rightarrow(\forall x_i)\,\mathscr{A}(x_i))$$

Así pues, por la Proposición 4.15, tenemos

$$\vdash_K((\forall x_i)\,\mathscr{A}(x_i)\leftrightarrow(\forall x_j)\,\mathscr{A}(x_j))$$

▷Esta proposición demuestra que podemos reemplazar una variable ligada particular, obteniendo una *fbf* cuya equivalencia con la original es demostrable, supuesto que escojamos la nueva variable adecuadamente. La utilidad de este procedimiento se hará patente más adelante.

Proposición 4.19

Sea $\mathscr{A}$ una *fbf* de $\mathscr{L}$ cuyas variables libres son $y_1, \ldots, y_n$. Entonces, $\vdash_K\mathscr{A}$ si y sólo si $\vdash_K(\forall y_1)\ \ldots\ (\forall y_n)\mathscr{A}$.

Demostración: Supongamos primero que $\vdash_K\mathscr{A}$. Procedemos por inducción sobre n, el número de variables libres de $\mathscr{A}$.

Paso base: $n=1$ (el caso de una fórmula sin variables libres es trivial). $\mathscr{A}$ tiene una variable, y_1. Si $\vdash_K\mathscr{A}(y_1)$ entonces $\vdash_K(\forall y_1)\mathscr{A}(y_1)$, mediante una simple aplicación de la regla de Generalización.

Paso de inducción: Sea $n>1$, y supongamos que el resultado es verdadero para toda *fbf* de $\mathscr{L}$ con $n-1$ variables libres. Consideremos la *fbf* $(\forall y_n)\,\mathscr{A}$. Esta tiene $n-1$ variables libres. Tenemos $\vdash_K\mathscr{A}$, luego $\vdash_K(\forall y_n)\,\mathscr{A}$, por Generalización, luego $\vdash_K(\forall y_1)\ \ldots\ (\forall y_{n-1})(\forall y_n)\,\mathscr{A}$, por hipótesis de inducción.

Recíprocamente, supongamos que $\vdash_K(\forall y_1)\ \ldots\ (\forall y_n)\mathscr{A}$ se demuestra análogamente por inducción sobre n, aplicando el axioma $(K5)$.

Definición 4.20

Si $\mathscr{A}$ es una *fbf* de $\mathscr{L}$ que contenga intervenciones libres de las variables $y_1, \ldots, y_n$, únicamente, entonces la *fbf* $(\forall y_1)\ldots(\forall y_n)\,\mathscr{A}$ se llama *cierre universal* de $\mathscr{A}$. El cierre universal de $\mathscr{A}$ suele denotarse por $\mathscr{A}'$.

Observación 4.21

Las proposiciones anteriores afirman que para toda *fbf* $\mathscr{A}$ de $\mathscr{L}$, $\vdash_K \mathscr{A}$ si y sólo si $\vdash_K \mathscr{A}'$. No obstante, convendrá que recordemos que $\mathscr{A}$ y $\mathscr{A}'$ no son en general demostrablemente equivalentes. No es difícil demostrar que $\vdash_K (\mathscr{A}' \rightarrow \mathscr{A})$ se cumple siempre, pero hemos visto en el Ejemplo 4.7 que $(\mathscr{A} \rightarrow \mathscr{A}')$ no es necesariamente un teorema de *K*.

Proposición 4.22

Sean $\mathscr{A}$ y $\mathscr{B}$ *fbfs* de $\mathscr{L}$, y supongamos que $\mathscr{B}_0$ resulta de la *fbf* $\mathscr{A}_0$ sustituyendo $\mathscr{B}$ en el lugar de una o más apariciones de $\mathscr{A}$ en $\mathscr{A}_0$. Entonces

$$\vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \rightarrow (\mathscr{A}_0 \leftrightarrow \mathscr{B}_0))$$

Demostración: Por inducción sobre la longitud de (es decir, el número de intervenciones de conectivas y cuantificadores en) $\mathscr{A}_0$.

Paso base: Estamos suponiendo, necesariamente, que $\mathscr{A}_0$ contiene a $\mathscr{A}$ como subfórmula. Por lo tanto, $\mathscr{A}_0$ contiene el mínimo de conectivas y cuantificadores cuando $\mathscr{A}_0$ es la propia $\mathscr{A}$. En este caso, $\mathscr{B}_0$ es precisamente $\mathscr{B}$. Entonces, $\vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \rightarrow (\mathscr{A} \leftrightarrow \mathscr{B}))$ es un caso particular de un resultado general mencionado en la Observación 4.21 de más arriba.

Paso de inducción: Supongamos que $\mathscr{A}_0$ contiene a $\mathscr{A}$ como subfórmula estricta, y que el resultado es verdadero para todas las *fbfs* de longitud menor que $\mathscr{A}_0$ y que contienen a $\mathscr{A}$ como subfórmula. Lo mismo que en otras demostraciones vistas anteriormente, hay tres casos por considerar:

Caso 1: $\mathscr{A}_0$ es $\sim \mathscr{C}_0$. Entonces $\mathscr{B}_0$ es $\sim \mathscr{D}_0$, siendo $\mathscr{D}_0$ el resultado de sustituir $\mathscr{B}$ en lugar de $\mathscr{A}$ en $\mathscr{C}_0$. Ahora bien, $\mathscr{C}_0$ tiene un número de conectivas y cuantificadores menor que $\mathscr{A}_0$, así que

$$\vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \rightarrow (\mathscr{C}_0 \leftrightarrow \mathscr{D}_0))$$

Como $((\mathscr{C}_0 \leftrightarrow \mathscr{D}_0) \rightarrow (\sim \mathscr{C}_0 \leftrightarrow \sim \mathscr{D}_0))$ es una tautología, es un teorema de *K*, y por *SH* (Corolario 4.10) tenemos:

$$\vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \rightarrow (\sim \mathscr{C}_0 \leftrightarrow \sim \mathscr{D}_0))$$

es decir,

$$\vdash_K ((\mathscr{A} \leftrightarrow \mathscr{B})' \rightarrow (\mathscr{A}_0 \leftrightarrow \mathscr{B}_0))$$

Caso 2: $\mathscr{A}_0$ es $(\mathscr{C}_0 \rightarrow \mathscr{D}_0)$. Entonces, $\mathscr{B}_0$ es $(\mathscr{E}_0 \rightarrow \mathscr{F}_0)$, siendo $\mathscr{E}_0$ y $\mathscr{F}_0$ los resultados de sustituir $\mathscr{B}$ en el lugar de $\mathscr{A}$ en $\mathscr{C}_0$ y $\mathscr{D}_0$, respec-

tivamente. Tanto $\mathscr{C}_0$ como $\mathscr{D}_0$ tienen ahora un número de conectivas y cuantificadores menor que el de $\mathscr{A}_0$, de modo que

$$\vdash_{\overline{K}}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{C}_0\leftrightarrow\mathscr{E}_0))$$

y

$$\vdash_{\overline{K}}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{D}_0\leftrightarrow\mathscr{F}_0))$$

Se deja como ejercicio el comprobar que de aquí se deduce que

$$\vdash_{\overline{K}}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow((\mathscr{C}_0\rightarrow\mathscr{D}_0)\leftrightarrow(\mathscr{E}_0\rightarrow\mathscr{F}_0)))$$

es decir,

$$\vdash_{\overline{K}}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{A}_0\leftrightarrow\mathscr{B}_0))$$

Caso 3: $\mathscr{A}_0$ es $(\forall x_i)\mathscr{C}_0$. Entonces $\mathscr{B}_0$ es $(\forall x_i)\mathscr{D}_0$, siendo $\mathscr{D}_0$ el resultado de sustituir $\mathscr{B}$ en el lugar de $\mathscr{A}$ en $\mathscr{C}_0$. $\mathscr{C}_0$ tiene ahora un número de conectivas y cuantificadores menor que el de $\mathscr{A}_0$, así que

$$\vdash_{\overline{K}}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{C}_0\leftrightarrow\mathscr{D}_0))$$

Mediante Generalización obtenemos entonces

$$\vdash_{\overline{K}}(\forall x_i)((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{C}_0\leftrightarrow\mathscr{D}_0))$$

Ahora bien, x_i no aparece libre en $(\mathscr{A}\leftrightarrow\mathscr{B})'$, luego como caso particular del axioma $(K6)$ se tiene

$$\vdash_{\overline{K}}((\forall x_i)((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{C}_0\leftrightarrow\mathscr{D}_0))\rightarrow((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\forall x_i)(\mathscr{C}_0\leftrightarrow\mathscr{D}_0)))$$

Así pues, por MP,

$$\vdash_{\overline{K}}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\forall x_i)(\mathscr{C}_0\leftrightarrow\mathscr{D}_0))$$

con lo que obtenemos nuestro resultado

$$\vdash_{\overline{K}}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow((\forall x_i)\mathscr{C}_0\leftrightarrow(\forall x_i)\mathscr{D}_0))$$

es decir,

$$\vdash_{\overline{K}}((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{A}_0\leftrightarrow\mathscr{B}_0)),$$

aplicando el siguiente lema, cuya demostración se deja como ejercicio.

Lema: Si $\mathscr{A}$ y $\mathscr{B}$ son *fbfs* de $\mathscr{L}$, entonces

$$\vdash_{\overline{K}}(\forall x_i)(\mathscr{A}\leftrightarrow\mathscr{B})\rightarrow((\forall x_i)\mathscr{A}\leftrightarrow(\forall x_i)\mathscr{B})$$

Esto completa nuestra demostración por inducción.

Corolario 4.23

Sean $\mathscr{A}$, $\mathscr{B}$, $\mathscr{A}_0$, $\mathscr{B}_0$ como en la Proposición 4.22. Si $\vdash_{\overline{K}}(\mathscr{A}\leftrightarrow\mathscr{B})$ entonces $\vdash_{\overline{K}}(\mathscr{A}_0\leftrightarrow\mathscr{B}_0)$.

Demostración: Supongamos que $\vdash_K(\mathscr{A}\leftrightarrow\mathscr{B})$. Entonces $\vdash_K(\mathscr{A}\leftrightarrow\mathscr{B})'$, por la Proposición 4.19. Por la Proposición 4.22, $\vdash_K((\mathscr{A}\leftrightarrow\mathscr{B})'\rightarrow(\mathscr{A}_0\leftrightarrow\mathscr{B}_0))$. Así pues, por MP, tenemos que $\vdash_K(\mathscr{A}_o\leftrightarrow\mathscr{B}_0)$

Corolario 4.24

Si x_j no aparece (ni libre ni ligada) en la *fbf* $\mathscr{A}(\mathbf{x}_i)$, y si la *fbf* $\mathscr{B}_0$ resulta de $\mathscr{A}_0$ reemplazando una o más intervenciones de $(\forall x_i)\mathscr{A}(x_i)$ por intervenciones de $(\forall x_j)\mathscr{A}(x_j)$, entonces $\vdash_K(\mathscr{A}_0\leftrightarrow\mathscr{B}_0)$

Demostración: Aplíquense la Proposición 4.18 y el Corolario 4.23.

Ejercicios

4 Demuéstrese que

$$\vdash_K((\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})\rightarrow((\forall x_i)\mathscr{A}\rightarrow(\forall x_i)\mathscr{B})),$$

cualesquiera que sean las *fbfs* $\mathscr{A}$ y $\mathscr{B}$.

5 Demuéstrese que la equivalencia de las *fbfs* $\sim(\exists x_i)\mathscr{A}$ y $(\forall x_i)(\sim\mathscr{A})$ es demostrable en K, cualquiera que sea la *fbf* $\mathscr{A}$ de $\mathscr{L}$.

6 Demuéstrese con detalle que

(*a*) $(\forall x_1)(\forall x_2)A_1^2(x_1, x_2)\vdash_K(\forall x_2)(\forall x_3)A_1^2(x_2, x_3)$.

(*b*) $(\forall x_1)(\forall x_2)A_1^2(x_1, x_2)\vdash_K(\forall x_1)A_1^2(x_1, x_1)$.

7 Sea $\mathscr{A}(x_i)$ una *fbf* de $\mathscr{L}$ en la que aparece libre x_i y sea x_j una variable que no aparece ni libre ni ligada en $\mathscr{A}(x_i)$. Demuéstrese que

$$\vdash_K((\exists x_i)\mathscr{A}(x_i)\leftrightarrow(\exists x_j)\mathscr{A}(x_j))$$

4.3. Forma prenexa

En el Capítulo 1 se introdujo la idea de forma normal y se discutieron las formas normales disyuntiva y conjuntiva. Uno de los usos de las formas normales es el sacar a la luz relaciones en la estructura lógica que pueden no ser obvias en las fórmulas originales. Ahora estamos en condiciones de describir una forma normal para *fbfs* de $\mathscr{L}$, y de la misma manera que en las formas normales consideradas anteriormente solamente permitíamos que ciertas conectivas se usasen de una manera standard, aquí nos va a importar la disposición de los cuantificadores.

Proposición 4.25

Sean $\mathscr{A}$ y $\mathscr{B}$ *fbfs* de $\mathscr{L}$.

(i) Si x_i no aparece libre en $\mathscr{A}$, entonces

$$\vdash_K((\forall x_i)(\mathscr{A}\to\mathscr{B})\leftrightarrow(\mathscr{A}\to(\forall x_i)\mathscr{B})),$$

y

$$\vdash_K((\exists x_i)(\mathscr{A}\to\mathscr{B})\leftrightarrow(\mathscr{A}\to(\exists x_i)\mathscr{B})).$$

(ii) Si x_i no aparece libre en $\mathscr{B}$, entonces

$$\vdash_K((\forall x_i)(\mathscr{A}\to\mathscr{B})\leftrightarrow((\exists x_i)\mathscr{A}\to\mathscr{B})),$$

y

$$\vdash_K((\exists x_i)(\mathscr{A}\to\mathscr{B})\leftrightarrow((\forall x_i)\mathscr{A}\to\mathscr{B}))$$

Demostración: Se necesitan ocho demostraciones en K. Una de ellas es trivial, por ser la *fbf* en cuestión un caso particular del axioma ($K6$); otra se ha dado ya en el Ejemplo 4.12, y otra se deduce fácilmente del Ejemplo 4.13. Las restantes requieren demostraciones similares, haciendo uso repetido del Teorema de Deducción. Se dejan como ejercicios.

Ejemplo 4.26

Demuéstrese que la *fbf*

$$(\forall x_1)A_1^1(x_1)\to(\forall x_2)(\exists x_3)A_1^2(x_2, x_3)$$

es demostrable equivalente a la *fbf*

$$(\exists x_1)(\forall x_2)(\exists x_3)(A_1^1(x_1)\to A_1^2(x_2, x_3)).$$

Escribimos una sucesión de *fbfs*, cada una de las cuales es demostrablemente equivalente a la siguiente, usando en cada paso una parte de la Proposición 4.25.

$$\begin{array}{l}(\forall x_1)A_1^1(x_1)\to(\forall x_2)(\exists x_3)A_1^2(x_2, x_3),\\ (\exists x_1)(A_1^1(x_1)\to(\forall x_2)(\exists x_3)A_1^2(x_2, x_3)),\\ (\exists x_1)(\forall x_2)(A_1^1(x_1)\to(\exists x_3)A_1^2(x_2, x_3)),\\ (\exists x_1)(\forall x_2)(\exists x_3)(A_1^1(x_1)\to A_1^2(x_2, x_3)).\end{array}$$

▷ Las *fbfs* de $\mathscr{L}$ pueden ser muy complicadas, y los cuantificadores que aparecen en ellas pueden ser difíciles de relacionar intuitivamente, en especial si están separadas. Podemos utilizar los resultados vistos anteriormente sobre sustitución y equivalencia para demostrar que toda *fbf* es demostrablemente equivalente a una en la que todos los cuantificadores aparecen al comienzo.

Definición 4.27

Una *fbf* $\mathscr{A}$ de $\mathscr{L}$ se dice que está en *forma prenexa* si es de la forma

$$(Q_1 x_{i1})(Q_2 x_{i2}) \ldots (Q_k x_{ik})\mathscr{D},$$

siendo $\mathscr{D}$ una *fbf* de $\mathscr{L}$ sin cuantificadores y donde cada Q_j es $\forall$ o $\exists$. (Una *fbf* sin cuantificadores se considera como un caso trivial de *fbf* en forma prenexa.)

Proposición 4.28

Para toda *fbf* $\mathscr{A}$ de $\mathscr{L}$ existe una *fbf* $\mathscr{B}$ que está en forma prenexa y es demostrablemente equivalente a $\mathscr{A}$.

Demostración: Por la Proposición 4.18, podemos cambiar todas las variables ligadas de $\mathscr{A}$ para hacerlas diferentes de las variables libres de $\mathscr{A}$ (dejando las variables libres inalteradas), obteniendo así una *fbf* $\mathscr{A}_1$ tal que $\vdash_K(\mathscr{A}_1 \leftrightarrow \mathscr{A})$. Ahora procedemos por inducción sobre la longitud de $\mathscr{A}_1$, es decir, el número de conectivas y cuantificadores que intervienen en $\mathscr{A}_1$.

Paso base: $\mathscr{A}_1$ es una fórmula atómica. En este caso no hay nada que demostrar, pues $\mathscr{A}_1$ está trivialmente en forma prenexa.

Paso de inducción: Supongamos que $\mathscr{A}_1$ no es una fórmula atómica y que toda *fbf* de longitud menor que $\mathscr{A}_1$ es demostrablemente equivalente a una *fbf* en forma prenexa. Hay tres casos:

Caso 1: $\mathscr{A}_1$ es $\sim\mathscr{C}$. Entonces $\mathscr{C}$ es de menor longitud que $\mathscr{A}_1$, de modo que existe una *fbf* $\mathscr{C}_1$ en forma prenexa, tal que $\vdash_K(\mathscr{C}_1 \leftrightarrow \mathscr{C})$. Se deduce que $\vdash_K (\mathscr{A}_1 \leftrightarrow (\sim\mathscr{C}_1))$, es decir, por ejemplo,

$$\vdash_K(\mathscr{A}_1 \leftrightarrow \sim(Q_1 x_{i_1}) \ldots (Q_k x_{i_k})\mathscr{D}).$$

De este modo, $\vdash_K \mathscr{A}_1 \leftrightarrow (Q_1^* x_{i_1}) \ldots (Q_k^* x_{i_k})(\sim\mathscr{D}))$, donde Q_j^* es $\exists$ si Q_j es $\forall$ y Q_j^* es $\forall$ si Q_j es $\exists$, para $1 \leqslant j \leqslant k$. Sea $\mathscr{B}$ la $fbf\,(Q_1^* x_{i_1}) \ldots (Q_k^* x_{i_k})(\sim\mathscr{D})$.

Entonces $\vdash_K(\mathscr{A} \leftrightarrow \mathscr{B})$, y $\mathscr{B}$ está en forma prenexa.

Caso 2. $\mathscr{A}_1$ es $(\mathscr{C} \to \mathscr{D})$. Entonces $\mathscr{C}$ y $\mathscr{D}$ son de menor longitud que $\mathscr{A}_1$, por lo que existen *fbfs* $\mathscr{C}_1$ y $\mathscr{D}_1$ en forma prenexa tales que

$$\vdash_K(\mathscr{C}_1 \leftrightarrow \mathscr{C}) \text{ y } \vdash_K(\mathscr{D}_1 \leftrightarrow \mathscr{D})$$

Entonces, por el Corolario 4.23

$$\vdash_K(\mathscr{C} \to \mathscr{D}) \leftrightarrow (\mathscr{C}_1 \to \mathscr{D}).$$

luego, por el mismo corolario y el Corolario 4.17

$$\vdash_K(\mathscr{C} \to \mathscr{D}) \leftrightarrow (\mathscr{C}_1 \to \mathscr{D}_1)$$

es decir,

$$\vdash_K (\mathscr{A}_1 \leftrightarrow (\mathscr{C}_1 \rightarrow \mathscr{D}_1))$$

Así pues, $\vdash_K (\mathscr{A} \leftrightarrow (\mathscr{C}_1 \rightarrow \mathscr{D}_1))$, por el Corolario 4.17. Ahora bien, $(\mathscr{C}_1 \rightarrow \mathscr{D}_1)$ tiene la forma

$$((Q_1 x_{i_1}) \ \ldots \ (Q_k x_{i_k})\mathscr{C}_2 \rightarrow (R_1 x_{j_1}) \ \ldots \ (R_l x_{jl})\mathscr{D}_2),$$

donde $\mathscr{C}_2$ y $\mathscr{D}_2$ no contienen cuantificadores y las Q_s y R_s son o $\forall$ o $\exists$. Aplicamos ahora repetidamente la Proposición 4.25 para llevar todos los cuantificadores al principio, cambiándolos en caso de ser necesario. Podemos hacerlo, puesto que $x_{i_1}, \ldots, x_{i_k}, x_{j_1}, \ldots, x_{j_1}$ son todas diferentes y distintas de cada una de las variables libres que figuran en $\mathscr{C}_2$ y $\mathscr{D}_2$. Obtenemos

$$\vdash_K ((\mathscr{C}_1 \rightarrow \mathscr{D}_1) \leftrightarrow (Q_1^* x_{i1}) \ \ldots \ (Q_k^* x_{ik})(R_1 x_{j1}) \ \ldots \ (Rlx_{jl})(\mathscr{C}_2 \rightarrow \mathscr{D}_2)).$$

Esta última parte es una *fbf* en forma prenexa, de manera que es la $\mathscr{B}$ requerida.

Caso 3: $\mathscr{A}_1$ es $(\forall x_i)\mathscr{C}$. Entonces la longitud de $\mathscr{C}$ es menor que la de $\mathscr{A}_1$ y existe una *fbf* en forma prenexa demostrablemente equivalente a $\mathscr{C}$. Supongamos

$$\vdash_K (\mathscr{C} \leftrightarrow (Q_1 x_{i_1}) \ \ldots \ (Q_k x_{ik})\mathscr{D}).$$

Entonces, por Generalización.

$$\vdash_K (\forall x_i)(\mathscr{C} \leftrightarrow (Q_1 x_{i1}) \ \ldots \ (Q_k x_{ik})\mathscr{D}),$$

y $\vdash_K ((\forall x_i)\mathscr{C} \leftrightarrow (\forall x_j)(Q_1 x_{i1} \ \ldots (Q_k x_{ik})\mathscr{D})$ se deduce como en la demostración de la Proposición 4.22. La *fbf* $(\forall x_i)(Q_1 x_{i1}) \ \ldots \ (Q_k x_{ik})\mathscr{D}$ es por tanto la $\mathscr{B}$ requerida.

Esto completa nuestra demostración por inducción.

Ejemplo 4.29

(*a*) Encuéntrese una *fbf* en forma prenexa que sea demostrablemente equivalente a la *fbf*

$$A_1^1(x_1) \rightarrow (\forall x_2) A_1^2(x_1, x_2)$$

Este ejemplo corresponde al Caso 2 de la demostración inductiva anterior. Obsérvese primero que x_2 es la única variable libre y que x_2 no aparece libre en ningún lugar, por lo que no necesitamos cambiar variables. Podemos aplicar directamente la Proposición 4.25(i), viendo que

$$(\forall x_2)(A_1^1(x_1) \rightarrow A_1^2(x_1, x_2))$$

es demostrablemente equivalente a la *fbf* dada, y está en forma prenexa.

(*b*) Encuéntrese una *fbf* en forma prenexa que sea demostrablemente equivalente a la *fbf*

$$(((\forall x_1)A_1^2(x_1, x_2)\rightarrow\sim(\exists x_2)(A_1^1(x_2))\rightarrow(\forall x_1)(\forall x_2)A_2^2(x_1, x_2))$$

De nuevo seguimos el método de la demostración de la Proposición 4.28. Primeramente cambiamos las variables ligadas. No importa cómo lo hagamos, con tal de que las variables ligadas sean distintas unas de otras y distintas de las variables libres. Obtenemos (por ejemplo)

$$(((\forall x_1)A_1^2(x_1, x_2)\rightarrow\sim(\exists x_3)A_1^1(x_3))\rightarrow(\forall x_4)(\forall x_5)A_2^2(x_4, x_5)))$$

que es demostrablemente equivalente a la *fbf* dada. Procedemos ahora por pasos, usando diferentes casos de la demostración inductiva de más arriba. Tratamos primero los cuantificadores que están precedidos inmediatamente por $\sim$(Caso 1) obteniendo

$$(((\forall x_1)A_1^2(x_1, x_2)\rightarrow(\forall x_3)\sim A_1^1(x_3))\rightarrow(\forall x_4)(\forall x_5)A_2^2(x_4, x_5)).$$

Consideremos ahora las partes de la forma $(\mathscr{B}\rightarrow\mathscr{C})$ (Caso 2). Obtenemos una sucesión de *fbfs*, cada una demostrablemente equivalente a la siguiente, usando las diferentes partes de la Proposición 4.25.

$$((\forall x_3)((\forall x_1)A_1^2(x_1, x_2)\rightarrow\sim A_1^1(x_3))\rightarrow(\forall x_4)(\forall x_5)A_2^2(x_4, x_5)),$$

$$((\forall x_3)(\exists x_1)(A_1^2(x_1, x_2)\rightarrow\sim A_1^1(x_3))\rightarrow(\forall x_4)(\forall x_4{}^5)A_2^2(x_4, x_5)),$$

$$(\exists x_3)(\forall x_1)((A_1^2(x_1, x_2)\rightarrow\sim A_1^1(x_3))\rightarrow(\forall x_4)(\forall x_5)A_2^2(x_4, x_5)),$$

$$(\exists x_3)(\forall x_1)(\forall x_4)(\forall x_5)((A_1^2(x_1, x_2)\rightarrow\sim A_1^1(x_3))\rightarrow A_2^2(x_4, x_5)).$$

Esta última *fbf* está en forma prenexa y es demostrablemente equivalente a la *fbf* dada.

▷ Nótese que este procedimiento no conduce a una respuesta única. El orden en que los cuantificadores se llevan al comienzo es arbitrario. Por ejemplo, la *fbf*

$$(\forall x_4)(\forall x_5)(\forall x_1)(\exists x_3)((A_1^2(x_1, x_2)\rightarrow\sim A_1^1(x_3))\rightarrow A_2^2(x_4, x_5))$$

es también una posible respuesta para el ejemplo anterior. No obstante, el orden de los cuantificadores al principio de una fórmula en forma prenexa es relevante. Tan sólo en ciertos casos particulares puede cambiarse este orden, y generalmente de ciertas maneras tan sólo, si es que se quiere que la *fbf* resultante sea demostrablemente equivalente a la *fbf* original.

Las formas prenexas proporcionan una manera de medir la complejidad de *fbfs* de K. Podría parecer a primera vista que para una *fbf*

en forma prenexa, la interpretación será tanto más compleja cuantos más cuantificadores haya al principio. No obstante, consideremos las dos *fbfs*

$$(\forall x_1)(\forall x_2)(\forall x_3)(\forall x_4)A_1^2(f_1^2(x_1, x_2), f_1^2(x_3, x_4)),$$
$$(\forall x_1)(\exists x_2)(\forall x_3)(\exists x_4)A_1^2(f_1^2(x_1, x_2), f_1^2(x_3, x_4)).$$

Podemos ver que la primera se interpreta mucho más fácilmente. Por ejemplo, consideremos la interpretación aritmética del Capítulo 3. Las interpretaciones de estas *fbfs* son respectivamente

para todo x, y, z, $t \in D_N$, $x+y=z+t$,

y para todo $x \in D_N$ existe algún $y \in D_N$ tal que para todo $x \in D_N$ existe algún $t \in D_N$ tal que $x+y=z+t$

El segundo enunciado es mucho más complicado, y es difícil ver a primera vista si es verdadero o falso. Las complicaciones aparecen a causa de los cuantificadores alternados, y el número de alternaciones es una medida de la complejidad.

Definición 4.30

(i) Sea $n>0$. Una *fbf* en forma prenexa es una forma Π_n si comienza con un cuantificador universal y tiene $n-1$ alternaciones de cuantificadores.

(ii) Sea $n>0$. Una *fbf* en forma prenexa es una forma Σ_n si comienza con un cuantificador existencial y tiene $n-1$ alteraciones de cuantificadores.

Nosotros no usaremos estas definiciones, pero son importantes en estudios más avanzados de la materia.

Ejemplo 4.31

(*a*) $(\forall x_1)(\forall x_2)(\exists x_3)A_1^3(x_1, x_2, x_3)$ es una forma Π_2.
(*b*) $(\forall x_1)(A_1^1(x_1) \rightarrow A_2^1(x_2))$ es una forma Π_1.
(*c*) $(\exists x_1)(\forall x_2)(\exists x_3)(\exists x_4)(A_1^2(x_1, x_2) \rightarrow A_1^2(x_3, x_4))$ es una forma Σ_3.

Ejercicios

8 Para cada una de las siguientes fórmulas, encuéntrese una fórmula en forma prenexa que sea demostrablemente equivalente a ella.

(*a*) $(\forall x_1)A_1^1(x_1)\rightarrow(\forall x_2)A_1^2(x_1, x_2)$.
(*b*) $(\forall x_1)(A_1^2(x_1, x_2)\rightarrow(\forall x_2)A_1^2(x_1, x_2))$.
(*c*) $(\forall x_1)(A_1^1(x_1)\rightarrow A_1^2(x_1, x_2))\rightarrow((\exists x_2)A_1^1(x_2)\rightarrow(\exists x_3)A_1^2(x_2, x_3))$.
(*d*) $(\exists x_1)A_1^2(x_1, x_2)\rightarrow(A_1^1(x_1)\rightarrow\sim(\exists x_3)A_1^2(x_1, x_3))$.

9 Sea $\mathscr{A}(x_1)$ una *fbf* en la que no aparece x_2, y sea $\mathscr{B}(x_2)$ una *fbf* en la que no aparece x_1. Supóngase que ni $\mathscr{A}$ ni $\mathscr{B}$ contienen cuantificadores. Demuéstrese que la fórmula

$$((\exists x_1)\mathscr{A}(x_1)\rightarrow(\exists x_2)\mathscr{B}(x_2))$$

es demostrablemente equivalente a fórmulas en forma prenexa de forma Π_2 y Σ_2.

10 Encuéntrese una fórmula en forma Π_3 que sea demostrablemente equivalente a una fórmula en forma Σ_2.

4.4 El Teorema de Adecuación para K

Vamos a llegar a demostrar la proposición siguiente:

Si $\mathscr{A}$ es una *fbf* lógicamente válida de $\mathscr{L}$, entonces $\mathscr{A}$ es un teorema de $K_{\mathscr{L}}$. No obstante, antes de llegar a la demostración, necesitamos algún trabajo preliminar que nos permita extender y aplicar las ideas empleadas en la demostración del Teorema de Adecuación para L.

En primer lugar, la idea de extensión puede generalizarse fácilmente. (Aquí, al igual que antes, escribimos K en lugar de $K_{\mathscr{L}}$, salvo que deseemos hacer énfasis en el lenguaje que se está utilizando.)

Definición 4.32

Una *extensión* de K es un sistema formal obtenido modificando o ampliando el conjunto de axiomas de tal manera que todos los teoremas de K permanezcan como tales (pudiendo aparecer eventualmente nuevos teoremas). Análogamente, dadas dos extensiones de K, una es extensión de la otra si su clase de teoremas es mayor (o, en el sentido trivial, la misma).

Definición 4.33

Un *sistema de primer orden* es una extensión de $K_{\mathscr{L}}$, para algún lenguaje de primer orden $\mathscr{L}$.

Definición 4.34

Un sistema de primer orden S es *consistente* si para ninguna *fbf* $\mathscr{A}$ se tiene que tanto $\mathscr{A}$ como $(\sim\mathscr{A})$ son teoremas de S.

Proposición 4.35. (Véase Proposición 2.19.)

Sea S un sistema de primer orden consistente y sea $\mathscr{A}$ una *fbf cerrada* que no es teorema de S. Entonces, S^* es también consistente, siendo S^* la extensión de S obtenida incluyendo $(\sim\mathscr{A})$ como axioma adicional.

Demostración: Supongamos que S^* es inconsistente. Entonces, para alguna *fbf* $\mathscr{B}$, $\vdash_{S^*}\mathscr{B}$ y $\vdash_{S^*}(\sim\mathscr{B})$. Ahora bien, $\vdash_{S^*}(\sim\mathscr{B}\rightarrow(\mathscr{B}\rightarrow\mathscr{A}))$por Proposición 4.3, ya que S^* es una extensión de K. Así pues, $\vdash_{S^*}(\mathscr{B}\rightarrow\mathscr{A})$ por MP, y $\vdash_{S^*}\mathscr{A}$ de nuevo por MP.

Existe pues una demostración de $\mathscr{A}$ en S^*. Una tal demostración es una deducción en S a partir de $(\sim\mathscr{A})$, luego tenemos

$$(\sim\mathscr{A})\vdash_S\mathscr{A}$$

Como $(\sim\mathscr{A})$ es cerrada, podemos aplicar el Teorema de Deducción, obteniendo

$$\vdash_S((\sim\mathscr{A})\rightarrow\mathscr{A})$$

Pero

$$\vdash_S(((\sim\mathscr{A})\rightarrow\mathscr{A})\rightarrow\mathscr{A}) \text{ por Proposición 4.3.}$$

Luego $\vdash_S\mathscr{A}$ por MP.

Esto contradice la hipótesis de que $\mathscr{A}^*$ no es teorema de S; luego S^* tiene que ser consistente.

▷ Nótese que esta proposición es un análogo de la Proposición 2.19, pero que tenemos que imponer la condición de que $\mathscr{A}$ sea una *fbf* cerrada. Esto no será inconveniente a la hora de aplicar nuestro resultado.

Definición 4.36

Un sistema de primer orden S es *completo* si para toda *fbf* cerrada, o bien $\vdash_S\mathscr{A}$ o $\vdash_S(\sim\mathscr{A})$.

Nótese que K *no* es completo. Por ejemplo, la *fbf* $(\forall x_1)A_1^1(x_1)$ no es teorema de K, ni tampoco lo es su negación.

Proposición 4.37 (Véase Proposición 2.21)

Sea S un sistema de primer orden consistente. Entonces existe una extensión consistente de S que es completa.

Demostración: La demostración sigue justamente el mismo patrón que

la demostración de la Proposición 2.21. Sea $\mathscr{A}_0$, $\mathscr{A}_1$, ... una enumeración de todas las *fbfs* cerradas de $\mathscr{L}$. Construimos una sucesión S_0, S_1, ... de extensiones de K como sigue. Tomemos como S_0 a S. Para $n \geq 0$, si $\vdash_{\overline{S^n}\text{-T}} \mathscr{A}_{n-1}$, sea S_n igual a S_{n-1}, y si no $\vdash_{\overline{S^n}\text{-T}} \mathscr{A}_{n-1}$, sea S_n la extensión de S_{n-1} obtenida añadiendo $(\sim \mathscr{A}_{n-1})$ como nuevo axioma. Por la Proposición 4.35, está claro que cada S_n es una extensión consistente de K. Sea S_∞ el sistema de primer orden que tiene como axiomas a todas las *fbfs* que sean axioma de al menos un S_n. Justo como en la demostración de la Proposición 2.21 podemos demostrar que S_∞ es consistente y completo.

▷ Es en este punto donde nuestros métodos tienen que hacerse ahora sustancialmente distintos a los del Capítulo 2. Si 'tradujésemos' la Proposición 2.22 a la terminología del Cálculo de predicados, obtendríamos: Si S es un sistema de primer orden consistente, existe una interpretación de $\mathscr{L}$ en la que todo teorema de S es verdadero. De hecho, vamos a llegar a demostrar esto; pero la demostración es bastante difícil y requiere ideas nuevas.

Hasta ahora, el lenguaje $\mathscr{L}$ ha sido fijo, aunque arbitrario. En la siguiente demostración tendremos ocasión de ampliar el lenguaje añadiendo una lista infinita de nuevas constantes individuales b_0, b_1, ... Ciertamente, esto tendrá el efecto de introducir en K nuevas *fbfs*, nuevos axiomas y nuevos teoremas (por ejemplo, la nueva $fbf((\forall x_1) A_1^1(x_1) \rightarrow A_1^1(b_1))$ será un acioma del sistema con lenguaje ampliado). No obstante, si S es una extensión consistente de $K_{\mathscr{L}}$, el nuevo sistema S^+ obtenido como acaba de decirse ampliando el lengueje, es también consistente. Puesto que, si $\mathscr{A}$ y $(\sim \mathscr{A})$ fuesen ambas teoremas de S^+, sus demostraciones, sucesiones finitas de *fbfs*, contendrían sólo un número finito de símbolos de entre b_0, b_1, b_2, ... Estas demostraciones podrían convertirse entonces en demostraciones en S sustituyendo cada uno de estos símbolos por una variable que no aparezca en las demostraciones originales. Obtendríamos pues demostraciones en S de una *fbf* de $\mathscr{L}$ y de su negación, lo cual es imposible.

Proposición 4.38

Sea S una extensión consistente de $K_{\mathscr{L}}$. Entonces existe una interpretación de $\mathscr{L}$ en la que todo teorema de S es verdadero.

Demostración: Ampliemos el lenguaje añadiendo una sucesión b_0, b_1, b_2, ... de nuevas constantes individuales. Denotemos por $\mathscr{L}^+$ al nuevo lenguaje y por S^+ y K^+ los nuevos sistemas obtenidos a partir de S y $K_{\mathscr{L}}$, respectivamente. Entonces, S^+ es consistente, como hemos razonado más arriba. Partiendo de S^+, definamos una sucesión de sistemas

de primer orden S_0, S_1, ... como sigue. Primeramente, enumeremos en una lista todas las *fbfs* de $\mathscr{L}$ que contienen exactamente una variable libre; por ejemplo

$$\mathscr{F}_0(x_{i0}),\ \mathscr{F}_1(x_{i1}),\ \ldots$$

Por supuesto, x_{i0}, x_{i1}, ... no serán todas distintas. Escojamos ahora una subsucesión c_0, c_1, c_2, ... de la sucesión b_0, b_1, b_2, ..., de modo que

(1) c_0 no aparece en $\mathscr{F}_0(x_{i0})$,

y

(2) para $n>0$, $c_n \notin \{c_0, \ldots, c_{n-1}\}$ y c_n no aparece en ninguna de las fórmulas.
$\mathscr{F}_0(x_{i0}), \ldots, \mathscr{F}_n(x_{in})$.

Podemos hacer esto, ya que cada *fbf* puede contener a lo sumo un número finito de intervenciones de las b_i.

Para cada k, denotaremos por $\mathscr{G}_k$ a la *fbf*

$$(\sim(\forall x_{ik})\mathscr{F}_k(x_{ik}) \rightarrow \sim\mathscr{F}_k(c_k)).$$

Sea ahora S_0 igual a S^+. Sea S_1 la extensión de S_0 obtenida añadiendo $\mathscr{G}_0$ como nuevo axioma. Para cada $n>1$, sea S_n la extensión de S_{n-1} obtenida añadiendo $\mathscr{G}_{n-1}$ como nuevo axioma. Nuestro procedimiento va a consistir en demostrar que cada S_n es consistente, obtener un sistema consistente S_∞ a partir de la sucesión, y aplicar la Proposición 4.37 para obtener una extensión completa y consistente de S_∞. Esto nos permitirá construir la interpretación requerida.

S_0 es consistente. Sea $n \geqslant 0$ y supongamos que S_n es consistente, pero S_{n+1} no lo es. Entonces existe una *fbf* $\mathscr{A}$ de $\mathscr{L}^+$ tal que:

$$\vdash_{S_{n+1}} \mathscr{A} \qquad \text{y} \quad \vdash_{S_{n+1}} (\sim\mathscr{A}).$$

Ahora bien, $\vdash_{S_{n+1}} (\mathscr{A} \rightarrow (\sim\mathscr{A} \rightarrow \sim\mathscr{B}))$, ya que $(\mathscr{A} \rightarrow (\sim\mathscr{A} \rightarrow \sim\mathscr{B}))$ es una tautología, cualquiera que sea la *fbf* $\mathscr{B}$. Así, mediante dos aplicaciones de MP, obtenemos

$$\vdash_{S_{n+1}} (\sim\mathscr{B}), \text{ para toda } \textit{fbf}\ \mathscr{B}.$$

En particular

$$\vdash_{S_{n+1}} (\sim\mathscr{G}_n).$$

Ahora bien, una demostración en S_{n+1} no es más que una deducción en S_n a partir de $\mathscr{G}_n$, luego tenemos

$$\mathscr{G}_n \vdash_{S_n} (\sim\mathscr{G}_n)$$

$\mathscr{G}_n$ es cerrada, de manera que, por el Teorema de Deducción,

$$\vdash_{S_n} (\mathscr{G}_n \rightarrow (\sim\mathscr{G}_n)).$$

Se deduce ahora, como ya hemos visto antes, que

$$\vdash_{S_n} (\sim \mathscr{G}_n)$$

es decir,

$$\vdash_{S_n} \sim(\sim(\forall x_{i_n})\mathscr{F}_n(x_{i_n}) \rightarrow \sim \mathscr{F}_n(c_n)).$$

Pero

$$\vdash_{S_n} (\sim(\sim(\forall x_{i_n})\mathscr{F}_n(x_{i_n}) \rightarrow \sim \mathscr{F}_n(c_n)) \rightarrow \sim(\forall x_{i_n})\mathscr{F}_n(x_{i_n})).$$

y

$$\vdash_{S_n} (\sim(\sim(\forall x_{i_n})\mathscr{F}_n(x_{i_n}) \rightarrow \sim \mathscr{F}_n(c_n)) \rightarrow \mathscr{F}_n(c_n)),$$

ya que estas dos *fbfs* son casos particulares de tautologías. Así pues, por *MP*, se tiene

$$\vdash_{S_n} \sim(\forall x_{i_n})\mathscr{F}_n(x_{i_n}) \qquad \text{y} \qquad \vdash_{S_n} \mathscr{F}_n(c_n).$$

En la demostración de $\mathscr{F}_n(c_n)$, reemplacemos cada intervención de c_n por y, siendo y una variable que no aparezca en ningún otro lugar de la demostración. Obtenemos así una demostración en S_n de $\mathscr{F}_n(y)$, ya que c_n no aparece en ninguno de los axiomas $\mathscr{G}_0, \mathscr{G}_1, \ldots, \mathscr{G}_{n-1}$ a partir de los cuales se ha derivado $\mathscr{G}_n(c_n)$ en S_n. Por lo tanto

$$\vdash_{S_n} \mathscr{F}_n(y)$$

Así pues,

$$\vdash_{S_n} (\forall y)\mathscr{F}_n(y) \text{ por Generalización}$$

y así

$$\vdash_{S_n} (\forall x_{i_n})\mathscr{F}_n(x_{i_n}) \text{ por la Proposición 4.18}$$

Hemos contradecido la consistencia de S_n, de manera que debe tenerse: Si S_n es consistente también lo es S_{n+1}, para todo $n \geqslant 0$. Así pues, por inducción, S_n es consistente para todo n.

Sea S_∞ el sistema obtenido incluyendo como axiomas a todas las *fbfs* de $\mathscr{L}^+$ que sean axioma de al menos uno de los S_n. S_∞ es consistente, ya que en caso contrario podría deducirse una contradicción usando sólo un número finito de sus axiomas, con lo que dicha contradicción podría deducirse también en S_n para algún n.

Por la Proposición 4.37, S_∞ posee una extensión consistente y completa T.

El modo en que vamos a construir ahora nuestra interpretación es algo nuevo y quizá cause confusión. Hasta ahora hemos considerado interpretaciones cuyos dominios constaban de objetos matemáticos, tales como números naturales o enteros. No obstante, según la defini-

ción, sólo se requiere que el dominio sea un conjunto no vacío. Definimos una interpretación I de $\mathscr{L}^+$ como sigue:

(*a*) El dominio D_I es el conjunto de todos los *términos cerrados* de $\mathscr{L}^+$, es decir, términos que no contengan variables (es decir, todas las constantes individuales y todos los términos construidos a partir de ellas usando las letras de función).

(*b*) Las constantes individuales son sus propias interpretaciones.

(*c*) Dadas $d_1, \ldots, d_n \in D_I$, $\bar{A}_i^n(d_1, \ldots, d_n)$ se verifica si $\vdash_{\overline{T}} A_i^n(d_1, \ldots, d_n)$ y no se verifica si $\vdash_{\overline{T}} (\sim A_i^n(d_1, \ldots, d_n))$. Esto tiene sentido, porque T es completa y $A_i^n(d_1, \ldots, d_n)$ es una *fbf.* cerrada.

(*d*) Dadas $d_1, \ldots, d_n \in D_I$, $\bar{f}_i^n(d_1, \ldots, d_n)$ recibe el valor $f_i^n(d_1, \ldots, d_n)$. Nótese que como $d_1, \ldots, d_n$ son términos cerrados, $f_i^n(d_1, \ldots, d_n)$ también lo es. Esto define la interpretación I. Ahora hemos de demostrar que todo teorema de S es verdadero en I.

Lema: Para toda *fbf* cerrada $\mathscr{A}$ de $\mathscr{L}^+$, $\vdash_{\overline{T}} \mathscr{A}$ si y sólo si $I \models \mathscr{A}$.

Demostración: La demostración es por inducción sobre el número de conectivas y cuantificadores de $\mathscr{A}$.

Paso base: $\mathscr{A}$ es una fórmula atómica, por ejemplo $A_i^n(d_1, \ldots, d_n)$, siendo $d_1, \ldots, d_n$ necesariamente términos cerrados.

Si $\vdash_{\overline{T}} \mathscr{A}$, entonces $\vdash_{\overline{T}} A_i^n(d_1, \cdots d_n)$, luego $A_i^n(d_1, \ldots, d_n)$, *en* I, es decir, $I \models \mathscr{A}$. Análogamente, si $I \models \mathscr{A}$ podemos deducir que $\vdash_{\overline{T}} \mathscr{A}$.

Paso de inducción: Supongamos que $\mathscr{A}$ no es atómica y que el resultado se verifica para toda *fbf.* más corta que $\mathscr{A}$.

Caso 1: $\mathscr{A}$ es $(\sim\mathscr{B})$. Si $\vdash_{\overline{T}} \mathscr{A}$, entonces $\vdash_{\overline{T}} (\sim\mathscr{B})$. Se deduce que $\mathscr{B}$ no es teorema de T, ya que T es consistente, y con ello $\mathscr{B}$ no es verdadera en I, por hipótesis de inducción. Así pues, $(\sim\mathscr{B})$ es verdadera en I, pues $\mathscr{B}$ es cerrada; es decir, $I \models \mathscr{A}$. Recíprocamente, si $I \models \mathscr{A}$, entonces $I \models (\sim\mathscr{B})$ y $\mathscr{B}$ no es verdadera en I, con lo que $\mathscr{B}$ no es teorema de T, por la hipótesis de inducción. Como T es completo, $(\sim\mathscr{B})$ es entonces teorema de T, es decir, $\vdash_{\overline{T}} \mathscr{A}$.

Caso 2: $\mathscr{A}$ es $(\mathscr{B}\rightarrow\mathscr{C})$. Supongamos que $\mathscr{A}$ no es verdadera en I. Entonces $\mathscr{B}$ es verdadera y $\mathscr{C}$ es falsa. Por hipótesis de inducción se tiene entonces que $\vdash_{\overline{T}} \mathscr{B}$ y no $\vdash_{\overline{T}} \mathscr{C}$. Como T es completo, tenemos $\vdash_{\overline{T}} \mathscr{B}$ y $\vdash_{\overline{T}} (\sim\mathscr{C})$. Ahora bien, $\vdash_{\overline{T}} (\mathscr{B}\rightarrow((\sim\mathscr{C})\rightarrow\sim(\mathscr{B}\rightarrow\mathscr{C})))$, puesto que esta *fbf.* es un caso particular de una tautología, así que usando *MP* dos veces obtenemos

$$\vdash_{\overline{T}} \sim(\mathscr{B}\rightarrow\mathscr{C}), \text{ es decir, } \vdash_{\overline{T}} (\sim\mathscr{A}).$$

Como T es consistente, $\mathscr{A}$ no es entonces teorema de T.

Recíprocamente, supongamos que $\mathscr{A}$ no es teorema de T. Entonces $\vdash_{\overline{T}} (\sim\mathscr{A})$ por la completitud T, con lo que $\vdash_{\overline{T}} \sim(\mathscr{B}\rightarrow\mathscr{C})$. Pero $(\sim(\mathscr{B}\rightarrow\mathscr{C})\rightarrow\mathscr{B})$ y $(\sim(\mathscr{B}\rightarrow\mathscr{C})\rightarrow\sim\mathscr{C})$ son tautologías, de modo que tenemos

$$\vdash_{\overline{T}} \mathscr{B} \qquad \text{y} \qquad \vdash_{\overline{T}} (\sim \mathscr{C})$$

con lo cual

$$\vdash_{\overline{T}} \mathscr{B} \text{ y no } \vdash_{\overline{T}} \mathscr{C}, \text{ ya que } T \text{ es consistente.}$$

Por la hipótesis de inducción se tiene entonces

$$I \models \mathscr{B} \text{ y no } I \models \mathscr{C}.$$

Así, $\mathscr{B}$ es verdadera en I y $\mathscr{C}$ es falsa en I. Por la Observación 3.25(d) se tiene entonces que $(\mathscr{B} \rightarrow \mathscr{C})$ es falsa en I, luego no verdadera en I.

Caso 3: $\mathscr{A}$ es $(\forall x_i)\mathscr{B}(x_i)$. En primer lugar, si x_i no aparece libre en $\mathscr{B}$, $\mathscr{B}$ es cerrada, de modo que por hipótesis de inducción, $\vdash_{\overline{T}} \mathscr{B}$ si y sólo si $I \models \mathscr{B}$. Sabemos también que $\vdash_{\overline{T}} \mathscr{B}$ si y sólo si $\vdash_{\overline{T}} (\forall x_i)\mathscr{B}$, y que $I \models \mathscr{B}$ si y sólo si $I \models (\forall x_i)\mathscr{B}$. Así pues, en este caso, $\vdash_{\overline{T}} \mathscr{A}$ si y sólo si $I \models \mathscr{A}$.

En segundo lugar, si x_i aparece libre en $\mathscr{B}(x_i)$, entonces es la única variable libre en $\mathscr{B}(x_i)$, ya que $\mathscr{A}$ es cerrada. Así pues, $\mathscr{B}(x_i)$ es una de las *fbfs* de la sucesión $\mathscr{F}_0(x_{i_0})$, $\mathscr{F}_1(x_{i_1})$, ...; supongamos que $\mathscr{B}(x_i)$ es $\mathscr{F}_m(x_{i_m})$. Entonces $\mathscr{A}$ es $(\forall x_{i_m})\mathscr{F}_m(x_{i_m})$. Supongamos que $I \models \mathscr{A}$. Por la Proposición 4.4, tenemos (a partir del axioma ($K5$))

$$I \models ((\forall x_{i_m})\mathscr{F}_m(x_{i_m}) \rightarrow \mathscr{F}_m(c_m)).$$

Así pues, $I \models \mathscr{F}_m(c_m)$. Ahora bien, $\mathscr{F}_m(c_m)$ tiene menos conectivos y cuantificadores que $\mathscr{A}$, luego por hipótesis de inducción $\vdash_{\overline{T}} \mathscr{F}_m(c_m)$. Deseamos demostrar que $\vdash_{\overline{T}} \mathscr{A}$; supongamos lo contrario, es decir, $\vdash_{\overline{T}} (\sim \mathscr{A})$, por ser T completa; o sea:

$$\vdash_{\overline{T}} \sim (\forall x_{i_m})\mathscr{F}_m(x_{i_m}).$$

Pero

$$\vdash_{\overline{T}} (\sim \forall x_{i_m})\mathscr{F}_m(x_{i_m}) \rightarrow \sim \mathscr{F}_m(c_m)),$$

ya que $\mathscr{G}_m$ es un axioma de T. Así pues, por MP,

$$\vdash_{\overline{T}} (\sim \mathscr{F}_m(c_m)).$$

Esto contradice la consistencia de T, de modo que tiene que ser $\vdash_{\overline{T}} \mathscr{A}$, como se quería.

Recíprocamente, supongamos que $\vdash_{\overline{T}} \mathscr{A}$ y que $\mathscr{A}$ no es verdadera en I, es decir, no $I \models (\forall x_{i_m})\mathscr{F}_m(x_{i_m})$. Existe entonces un elemento d de D_I tal que $I \models (\sim \mathscr{F}_m(d))$. Para ver esto, obsérvese que existe una valoración en I que no satisface $(\forall x_{i_m})\mathscr{F}_m(x_{i_m})$, por lo que existe una valoración v que no satisface $\mathscr{F}_m(x_{i_m})$. Ahora bien, $v(x_{i_m}) \in D_I$, es decir, $v(x_{i_m})$ es un término cerrado, llamémosle d, y un término así necesariamente está libre para x_{i_m} en $\mathscr{F}_m(x_{i_m})$. Además, $v(d) = d$. Así pues, $v(x_{i_m}) = v(d)$. Por el resultado del Ejercicio 3.23 se tiene entonces que v

no satisface a $\mathscr{F}_m(d)$, por lo que $\mathscr{F}_m(d)$ no es verdadera en I. Así, $I \models (\sim \mathscr{F}_m(d))$, como se quería. Pero $\vdash_{\overline{T}} (\forall x_{im}) \mathscr{F}_m(x_{im})$, luego $\vdash_{\overline{T}} \mathscr{F}_m(d)$, por el axioma $(K5)$ y MP. Por la hipótesis de inducción se tiene entonces que $I \models \mathscr{F}_m(d)$. Pero $\mathscr{F}_m(d)$ y $\sim \mathscr{F}_m(d)$ no pueden ser ambas verdaderas en I, así que $\vdash_{\overline{T}} \mathscr{A}$ implica $I \models \mathscr{A}$ en este caso.

Esto completa la demostración inductiva del lema, con lo cual sabemos que todo teorema de T es verdadero en la interpretación I. Todo teorema de S es un teorema de T, ya que T se obtuvo a partir de S ampliando el lenguaje y añadiendo nuevos axiomas. Así pues, toda *fbf* de $\mathscr{L}^+$ que sea un teorema de S es verdadera en I. Por supuesto, todo teorema de S es una *fbf.* de $\mathscr{L}$ e I contiene interpretaciones de *fbfs* que no son de $\mathscr{L}$, así que restringiremos I excluyendo las interpretaciones de las constantes individuales b_0, b_1, ... y de los términos que dependen de ellas, pero dejando D_I sin modificar. Esto nos proporciona una interpretación de $\mathscr{L}$, en la cual es verdadero todo teorema de S.

▷ Aún no hemos demostrado el Teorema de Adecuación, pero el considerable esfuerzo que nos ha exigido la demostración de la Proposición 4.38 nos permitirá completar la demostración del Teorema de Adecuación con bastante facilidad.

Proposición 4.39 (El Teorema de Adecuación para $K_{\mathscr{L}}$)

Si $\mathscr{A}$ es una *fbf.* lógicamente válida de $\mathscr{L}$, entonces $\mathscr{A}$ es un teorema de $K_{\mathscr{L}}$.

Demostración: Sea $\mathscr{A}$ una *fbf.* lógicamente válida de $\mathscr{L}$ y sea $\mathscr{A}'$ su cierre universal. Se deduce del Corolario 3.28 que $\mathscr{A}'$ también es lógicamente válida. Supongamos que $\mathscr{A}$ no es un teorema de $K_{\mathscr{L}}$. Entonces, por la Proposición 4.19, $\mathscr{A}'$ no es un teorema de $K_{\mathscr{L}}$. Si incluimos $\sim \mathscr{A}'$ como axioma adicional, obtendremos un nuevo sistema $K'_{\mathscr{L}}$, que será consistente por la Proposición 4.35. Así pues, por la Proposición 4.38, hay una interpretación de $\mathscr{L}$ en la cual todo teorema de $K'_{\mathscr{L}}$ es verdadero. En particular, $\sim \mathscr{A}'$ es verdadera en esta interpretación, de manera que $\mathscr{A}'$ es falsa ($\mathscr{A}'$ es necesariamente cerrada). Esto contradice la validez lógica de $\mathscr{A}'$, con lo cual $\mathscr{A}$ tiene que ser un teorema de $K_{\mathscr{L}}$.

▷ Hemos completado la tarea que teníamos entre manos, habiendo demostrado que los teoremas de $K_{\mathscr{L}}$ son exactamente las *fbfs* lógicamente válidas de $\mathscr{L}$. A pesar de que la demostración de hecho nos ha causado algunas dificultades (la primera demostración la dio Gödel en 1930 y la demostración que nosotros hemos dado es una posterior, debida en esencia a Henkin), el resultado en sí no es sorprendente. El sistema $K_{\mathscr{L}}$ se construyó del modo en que se construyó precisamente

para hacer posible la demostración de todo lo que quepa esperar que sea demostrable mediante métodos de la lógica ordinaria o intuitiva, o sea, las 'verdades lógicas' (por ejemplo, las *fbfs.* lógicamente válidas). No obstante, el Teorema de Adecuación es un teorema central, ya que confirma que $K_{\mathscr{L}}$ hace lo que se esperaba de él.

Ejercicios

11 Demuéstrese que una extensión S de $K_{\mathscr{L}}$ es inconsistente si y sólo si toda *fbf* de $\mathscr{L}$ es un teorema de S.
12 Sea S un sistema de primer orden consistente tal que, para toda *fbf* cerrada $\mathscr{A}$ de S, si el sistema obtenido añadiendo $\mathscr{A}$ como axioma adicional es consistente, entonces $\mathscr{A}$ es un teorema de S. Demuéstrese que S es completo.
13 Sean $\mathscr{A}$ y $\mathscr{B}$ *fbfs* de $\mathscr{L}$ tales que $(\mathscr{A} \vee \mathscr{B})$ es un teorema de $K_{\mathscr{L}}$. ¿Ha de darse necesariamente el caso de que o $\mathscr{A}$ o $\mathscr{B}$ sea un teorema de $K_{\mathscr{L}}$?
14 Sea $\mathscr{L}$ un lenguaje de primer orden con infinitas letras de predicado. Demuéstrese que $K_{\mathscr{L}}$ tiene infinitas extensiones consistentes.

4.5 Modelos

La Proposición 4.39 tiene muchas consecuencias, de las cuales mencionaremos algunas aquí. Para hacerlo conviene introducir en este punto una nueva noción, la de modelo.

Definición 4.40

(i) Sea Γ un conjunto de *fbfs* de $\mathscr{L}$. Una interpretación de $\mathscr{L}$ en la que sea verdadero todo miembro de Γ se llama un *modelo* de Γ.
(ii) Si S es un sistema de primer orden, un *modelo* de S es una interpretación en la que sea verdadero todo teorema de S.

Proposición 4.41

Sea S un sistema de primer orden, y sea I una interpretación en la que sean verdaderos todos los axiomas de S. Entonces I es un modelo de S.

Demostración (cf. la demostración de la Proposición 4.5):

Supongamos que I es una interpretación en la que todos los axiomas de S son verdaderos. Sea $\mathscr{A}$ un teorema de S. Demostraremos

que $\mathscr{A}$ ha de ser verdadera en I por inducción sobre el número n de *fbfs* de una demostración de $\mathscr{A}$.

Paso base: $n=1$. $\mathscr{A}$ es un axioma de S, y por tanto verdadera en I.

Paso de inducción: $n>1$. Supongamos que todo teorema que posea una demostración más corta es verdadero en I.

Caso 1: $\mathscr{A}$ se deduce de *fbfs* anteriores de la demostración mediante *MP;* sean las *fbfs* anteriores $\mathscr{A}$ y $(\mathscr{B}\rightarrow\mathscr{A})$. Por la hipótesis de inducción, $\mathscr{B}$ y $(\mathscr{B}\rightarrow\mathscr{A})$ son verdaderas en I, de modo que, por la Proposición 3.26, $\mathscr{A}$ es verdadera en I.

Caso 2: $\mathscr{A}$ se deduce de una *fbfs.* anterior mediante Generalización. Supongamos que $\mathscr{A}$ es $(\forall x_i)\mathscr{B}$ y que la fórmula anterior es $\mathscr{B}$. Por hipótesis de inducción, $\mathscr{B}$ es verdadera en I, de modo que por la Proposición 3.27 $(\forall x_i)\mathscr{B}$ es verdadera en I.

Caso 3: $\mathscr{A}$ es un axioma de S. Del mismo modo que más arriba $\mathscr{A}$ es forzosamente verdadera en I.

Esto completa nuestra demostración inductiva de que todo teorema de S es verdadero en I. Se sigue que I es modelo de S.

$\triangleright$ Lo que hemos demostrado es que un modelo, en el sentido de la Definición 4.40(ii), de un sistema de primer orden S, es lo mismo que un modelo, en el sentido de la Definición 4.40(i), del conjunto de axiomas de S.

Nótese que es una consecuencia trivial de la Proposición 4.5 que toda interpretación de $\mathscr{L}$ es un modelo de $K_{\mathscr{L}}$, puesto que todo teorema de $K_{\mathscr{L}}$ es verdadero en toda interpretación. La noción de modelo es más importante en el contexto de extensiones de $K_{\mathscr{L}}$, en las cuales la clase de los teoremas es mayor y para las cuales existen interpretaciones que no son modelos.

La Proposición 4.38 puede ahora reformularse así: Si un sistema de primer orden S es consistente, entonces tiene un modelo. De hecho, tenemos la siguiente proposición:

Proposición 4.42

Un sistema de primer orden S es consistente si y sólo si tiene un modelo.

Demostración: Uno de los dos sentidos de la implicación ha sido demostrado ya. Supongamos que S tiene un modelo, por ejemplo I, y que S es inconsistente. Entonces $\vdash_S \mathscr{A}$ y $\vdash_S (\sim\mathscr{A})$ para alguna *fbf* $\mathscr{A}$. Ahora bien, todos los teoremas de S son verdaderos en el modelo I, así que $\mathscr{A}$ y $(\sim\mathscr{A})$ son ambas verdaderas en I. Esto es imposible, por la Observación 3.25(*b*), de modo que S ha de ser consistente.

Ejemplo 4.43

Sea $\mathscr{A}$ una *fbf* cerrada de $\mathscr{L}$ tal que ni $\mathscr{A}$ ni $(\sim\mathscr{A})$ sean teoremas de K. Entonces, por la proposición 4.35, los sistemas K^1 y K^2 poseen cada uno un modelo. El modelo de K^1 será una interpretación I_1 en la que $\mathscr{A}$ será verdadera. El modelo de K^2 será una interpretación I_2 en la que $(\sim\mathscr{A})$ será verdadera. Así pues, I_1 no puede ser modelo de K^2 y análogamente I_2 no puede ser modelo de K^1. Se deduce de esto que todo sistema de primer orden consistente que no sea completo es decir, en el que existe una *fbf* cerrada $\mathscr{A}$ tal que ni $\mathscr{A}$ ni $(\sim\mathscr{A})$ son teoremas) tiene al menos dos modelos esencialmente diferentes.

▷Debemos tener cuidado de evitar caer en la trampa de suponer que porque una cierta *fbf* sea verdadera en un modelo de un sistema S tiene que ser un teorema de S. El ejemplo anterior muestra que esto no tiene por qué cumplirse. No obstante, podemos avanzar algo en esta dirección, como consecuencia de la Proposición 4.42.

Proposición 4.44

Sea S un sistema de primer orden consistente y $\mathscr{A}$ una *fbf* cerrada que sea verdadera en todo *modelo* de S. Entonces $\mathscr{A}$ es un teorema de S.

Demostración: Sea $\mathscr{A}$ una *fbf* cerrada, verdadera en todo modelo de S, y supongamos que $\mathscr{A}$ no es un teorema de S. Entonces, por la Proposición 4.35, el sistema S' obtenido a partir de S incluyendo $(\sim\mathscr{A})$ como axioma adicional es consistente. S' tiene pues un modelo, digamos M, por la Proposición 4.42 $(\sim\mathscr{A})$ es verdadera en M, por lo que $\mathscr{A}$ es falsa en M. Pero M es un modelo de S (ya que S' es una extensión de S). Esto contradice la hipótesis de que $\mathscr{A}$ es verdadera en todo modelo de S, así que $\mathscr{A}$ debe ser un teorema de S.

Proposición 4.45 (Teorema de Löwenheim-Skolem)

Si un sistema de primer orden S tiene un modelo, entonces S tiene un modelo cuyo dominio es un conjunto numerable (un conjunto es numerable si sus elementos pueden ponerse en correspondencia biunívoca con el conjunto de los números naturales).

Demostración: Si S tiene un modelo, entonces S es consistente, por la Proposición 4.42, Si S es consistente, entonces la demostración de la Proposición 4.38 demuestra que S tiene un modelo de naturaleza particular: Su dominio es el conjunto de los términos cerrados de un lenguaje ampliado. Dicho conjunto es numerable. Ello puede demostrarse

describiendo un procedimiento para escribir una lista (infinita, por supuesto) que llegue a incluir a todos los términos cerrados. Esto puede hacerse de varias maneras y se deja como ejercicio.

▷ Esta proposición tiene algunas consecuencias sorprendentes, como veremos en un capítulo posterior.

Proposición 4.46 (Teorema de Compacidad)

Si todo subconjunto finito del conjunto de axiomas de un sistema de primer orden S tiene un modelo, entonces el propio S tiene un modelo.

Demostración: Supongamos que todo conjunto finito de axiomas de S tiene un modelo, pero que S no tiene modelos. Entonces S es inconsistente, por la Proposición 4.42. Así pues, $\vdash_S \mathscr{A}$ y $\vdash_S (\sim\mathscr{A})$, para alguna *fbf* $\mathscr{A}$. Pero estas demostraciones sólo pueden contener casos particulares de un número finito de axiomas de S. Sea Γ el conjunto de todos los axiomas de S que se usan en estas demostraciones. Γ es finito y tiene, por tanto, un modelo. Existe pues una interpretación I en la que es verdadero todo miembro de Γ. Se deduce que $\mathscr{A}$ y $(\sim\mathscr{A})$ tienen que ser ambas verdaderas en I. Esto es debido a que las reglas de deducción, *MP* y Generalización, preservan la verdad en una interpretación (véase la demostración de la Proposición 4.41). Pero $\mathscr{A}$ y $(\sim\mathscr{A})$ no pueden ser verdaderas las dos en I; hemos llegado a una contradicción, y S tiene que tener un modelo.

▷ Esta proposición se enuncia a veces de un modo ligeramente diferente, que damos como corolario.

Corolario 4.47)

Sea Γ un conjunto infinito de *fbfs*. de $K_{\mathscr{L}}$. Entonces, Γ tiene un modelo si todo subconjunto finito de Γ tiene un modelo.

▷ Hay un modo de producir sistemas de primer orden a partir de modelos. Sea S un sistema de primer orden y supongamos que S es consistente. Entonces tiene un modelo, llamémosle I. Supongamos que S no es completo, de manera que para alguna *fbf* cerrada $\mathscr{A}$, ni $\mathscr{A}$ ni $(\sim\mathscr{A})$ sean teoremas de S. No obstante, en I esta *fbf* $\mathscr{A}$ es o verdadera o falsa, es decir, o bien $I \models \mathscr{A}$ o $I \models (\sim A)$. Análogamente, el modelo I da un valor de verdad' a cada *fbf.* cerrada. Definamos un nuevo sistema de primer orden $S(I)$ incluyendo como axiomas todas las *fbfs* verdaderas en I. Entonces, los teoremas de $S(I)$ son todos axiomas de $S(I)$, puesto que cualquier consecuencia de *fbfs* verdaderas en I será

también verdadera en I. $S(I)$ es consistente, porque si $\vdash_{\overline{S(I)}} \mathscr{A}$ y $\vdash_{\overline{S(I)}} (\sim \mathscr{A})$ entonces $\mathscr{A}$ y $(\sim \mathscr{A})$ serían ambas verdaderas en I, lo que es imposible. Nótese que I es un modelo de $S(I)$. $S(I)$ es también completo, pues dada cualquier *fbf* cerrada $\mathscr{A}$, o $I \models \mathscr{A}$ o $I \models (\sim \mathscr{A})$ con lo que ciertamente tenemos que $\vdash_{\overline{S(I)}} \mathscr{A}$ o $\vdash_{\overline{S(I)}} (\sim \mathscr{A})$.

Ejercicios

15 Sea Γ un conjunto de *fbfs* de $\mathscr{L}$ y sea M un modelo de Γ. Demuéstrese que si $\Gamma \vdash_{\overline{K_{\mathscr{L}}}} \mathscr{A}$, entonces $\mathscr{A}$ es verdadera en M. ¿Se verifica también el recíproco?

16 Sea S una extensión consistente y completa de $K_{\mathscr{L}}$. Demuéstrese que dos modelos cualesquiera de S son elementalmente equivalentes, es decir, que toda *fbf* cerrada verdadera en uno de los dos modelos es verdadera en el otro.

17 Sea S una extensión consistente de $K_{\mathscr{L}}$ y sea M un modelo de S. Defínase una extensión S^+ de S como sigue: Inclúyanse como axiomas adicionales todas las fórmulas atómicas de $\mathscr{L}$ verdaderas en M. Demuéstrese que S^+ es consistente. ¿Es S^+ necesariamente completo?

18 Sea S una extensión consistente de $K_{\mathscr{L}}$ y sea M un modelo de S. Defínase una extensión $\hat{S}$ de S como sigue: Inclúyanse como axiomas adicionales todas las fórmulas atómicas *cerradas* de $\mathscr{L}$ verdaderas en M y las negaciones de todas las fórmulas atómicas *cerradas* de $\mathscr{L}$ falsas en M. Demuéstrese que $\hat{S}$ es consistente. ¿Es $\hat{S}$ necesariamente completo?

19 Sea S una extensión consistente de $K_{\mathscr{L}}$, siendo $\mathscr{L}$ el lenguaje de primer orden que contiene variables, constante individuales a_1, a_2, ... una sola letra de predicado A_1^1 y ninguna letra de función. Podemos imaginar una interpretación I de $\mathscr{L}$ como un conjunto D_I junto con un subconjunto distinguido A_I formado por todos los $x \in D_I$ tales que $\bar{A}_1^1(x)$ se verifica en I. Supongamos que para todo $n \geqslant 1$ existe un modelo M_n de S en el que $\bar{a}_i \in A_M$ para $1 \leqslant i \leqslant n$. Demuéstrese que existe un modelo M de S en el que $\bar{a}_i \in A_M$ para todo i.

5
Sistemas matemáticos

5.1 Introducción

Los capítulos 1 al 4 no son matemáticas. Los sistemas L y $K_{\mathscr{L}}$ son sistemas de deducción lógica. Hemos tenido que usar algunas técnicas matemáticas para obtener demostraciones de proposiciones, pero se ha tratado de técnicas de naturaleza elemental, principalmente propiedades de los números naturales. El matemático interesado en los fundamentos de su materia trata de clarificar las hipótesis que hace y los procedimientos que utiliza. Para este tipo de clarificación podemos usar el sistema $K_{\mathscr{L}}$. $K_{\mathscr{L}}$ comprende el tipo de procedimientos de deducción lógica que los matemáticos emplean. Ya hemos visto que la ausencia de restricciones acerca del lenguaje $\mathscr{L}$ hacen muy generales nuestros resultados acerca de $K_{\mathscr{L}}$, y que los símbolos de un $\mathscr{L}$ dado pueden interpretarse de muy diversas maneras. No obstante, para cualquier $\mathscr{L}$ existe una clase de *fbfs* cuya verdad no depende de la interpretación de los símbolos: La clase de las *fbfs* lógicamente válidas, es decir, la clase de los teoremas de $K_{\mathscr{L}}$. Si $\mathscr{L}$ se interpreta de un modo matemático, como ha ocurrido en nuestros ejemplos, los teoremas de $K_{\mathscr{L}}$ quedan interpretados como verdades matemáticas: Son enunciados matemáticos verdaderos a causa de su estructura lógica, más que a causa de su contenido matemático. Por ejemplo, en la interpretación aritmética N, la *fbf*

$$(\forall x_1)(\forall x_2)(A_1^2(x_1,\ x_2)\rightarrow A_1^2(x_1,\ x_2))$$

que es lógicamente válida, se interpreta como un enunciado matemático, concretamente: «para todos los números naturales x e y, si $x=y$ entonces $x=y'$, que es verdadero en virtud de su estructura lógica. Por otra parte, la *fbf*

$$(\forall x_1)(\forall x_2)(A_1^2(x_1,\ x_2)\rightarrow A_1^2(x_2,\ x_1))$$

se interpreta como el enunciado matemático: «para todos los números naturales x e y si $x=y$ entonces $y=x'$ que es verdadero. No obstante,

esta verdad es consecuencia del significado de «=» y no de la mera estructura lógica. De hecho, esta *fbf* no es lógicamente válida. No es difícil encontrar una interpretación en la cual A_1^1 no se interprete por $=$ y que haga falsa la *fbf*. Se deduce que esta *fbf* no es un teorema de $K_{\mathscr{L}}$. Así pues, los teoremas de $K_{\mathscr{L}}$ no tienen por sí mismos valor matemático. Cada uno de nuestros sistemas formales matemáticos va a ser una extensión de algún $K_{\mathscr{L}}$, obtenida añadiendo axiomas adicionales apropiados, de tal manera que los teoremas del sistema representan verdades matemáticas además de verdades lógicas. Si queremos que nuestro sistema formal sea un sistema matemático, está claro que es deseable el tener como teoremas a todas las *fbfs* cuyas interpretaciones sean verdades matemáticas (o, si esto no es posible, tantas de ellas como se pueda).

El qué constituye una verdad matemática, depende en gran medida del contexto matemático. Por ejemplo, el enunciado

$$(\forall x)(\forall y)(xy = yx)$$

es verdadero si se le considera como un enunciado acerca de números naturales, pero no es necesariamente verdadero si se le considera como un enunciado acerca de los elementos de un grupo arbitrario. Demostraremos mediante ejemplos cómo diferentes contextos matemáticos pueden ser representados por medio de diferentes sistemas formales de modo que, en particular, el enunciado anterior sería la interpretación de un teorema de la aritmética formal, y a la vez la interpretación de un no-teorema de la teoría de grupos formal. El contexto determinará el lenguaje $\mathscr{L}$ (como en el caso de la aritmética) y determinará también un conjunto de *axiomas propios*. La palabra «propio» se usa para distinguir a estos axiomas de (*K*1)-(*K*6), que son *axiomas lógicos*, comunes a todos los sistemas. Habiendo especificado $\mathscr{L}$, los axiomas propios son *fbfs*. de $\mathscr{L}$ que, añadidas como nuevos axiomas, dan una extensión de $K_{\mathscr{L}}$ en la cual las verdades matemáticas del contexto de que se trate (y también las verdades lógicas) aparecen como interpretaciones de teoremas.

5.2 Sistemas de primer orden con igualdad

En matemáticas es difícil prescindir de la relación de igualdad. El símbolo «=» no aparece en nuestros lenguajes formales, pero en algunos ejemplos lo hemos utilizado como interpretación del símbolo de predicado A_1^2. En nuestros ejemplos de sistemas matemáticos incluiremos A_1^2 en el lenguaje, y $=$ será la interpretación prevista para él. Como observamos antes, la *fbf*. $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2) \rightarrow A_1^2(x_2, x_1))$ no es un teorema de $K_{\mathscr{L}}$, pero nos gustaría que fuese un teorema de nuestras extensiones matemáticas de $K_{\mathscr{L}}$. Una manera de asegurar esto sería incluirla entre los axiomas propios de cada sistema matemático. Pero es

evidente que hay otras *fbfs* que podrían requerir un tratamiento similar; por ejemplo, $(\forall x_1)A_1^2(x_1, x_1)$. No necesitamos incluir como axiomas todas estas *fbfs*, sino que basta con que tomemos como *axiomas de la igualdad* un conjunto de ellas a partir del cual puedan deducirse las otras

(*E*7) $A_1^2(x_1, x_1)$.

(*E*8) $A_1^2(t_k,u) \rightarrow A_1^2(f_1^n(t_1, \ldots, t_k, \ldots, t_n), f_i^n(t_1, \ldots, u, \ldots, t_n))$, siendo $t_1, \ldots, t_n, u$ términos cualesquiera y f_i^n cualquier letra de función de $\mathscr{L}$.

(*E*9) $(A_1^2(t_k,u) \rightarrow (A_i^n(t_1, \ldots, t_k, \ldots, t_n) \rightarrow A_i^n(t_1, \ldots, u, \ldots, t_n)))$, siendo $t_1, \ldots, t_n, u$ términos cualesquiera y A_i^n cualquier símbolo de predicado de $\mathscr{L}$.

Notas 5.1

(*a*) (*E*8) y (*E*9) son esquemas de axiomas, cada uno de los cuales representa a un cierto número de axiomas, eventualmente infinitos, dependiendo del número de letras de función y de símbolos de predicado de $\mathscr{L}$.

(*b*) En todos estos axiomas intervienen variables. Se han escrito así para mayor claridad y para facilitar posteriores aplicaciones. No obstante, sabemos que para toda *fbf* $\mathscr{A}$ cuyo cierre universal sea $\mathscr{A}'$, $\mathscr{A} \mid\!\!-_{K_{\mathscr{L}}} \mathscr{A}'$ y $\mathscr{A}' \mid\!\!-_{K_{\mathscr{L}}} \mathscr{A}$, de manera que los cierres universales de los axiomas formarían un conjunto de axiomas equivalente.

(*c*) Como consecuencia de (*b*) y de la Proposición 4.18 referente al cambio de variables ligadas, el hecho de que sea la variable x_1 la que aparezca en (*E*7) no tiene mayor significación. Por ejemplo, $A_1^2(x_5, x_5)$ es consecuencia de (*E*7), mediante la deducción:

(1)	$A_1^2(x_1, x_1)$	(*E*7)
(2)	$(\forall x_1) A_1^2(x_1, x_1)$	(1), Generalización
(3)	$(\forall x_5) A_1^2(x_5, x_5)$	(2), Proposición 4.18
(4)	$(\forall x_5) A_1^2(x_5, x_5) \rightarrow A_1^2(x_5, x_5)$	(*K*5)
(5)	$A_1^2(x_5, x_5)$	(3), (4), *MP*

Todos los sistemas matemáticos que describiremos van a ser extensiones de $K_{\mathscr{L}}$ (para algún $\mathscr{L}$) que incluirán entre sus axiomas (*E*7) y todos los casos particulares adecuados (dependiendo de $\mathscr{L}$) de (*E*8) y (*E*9).

Observación 5.2

La necesidad de incluir (*E*7) debería estar clara. Nos asegura que en todo modelo la interpretación de A_1^2 se comporta en un sentido

como $=$. ($E8$) y ($E9$) son más complejos, pero su inclusión asegura que en cualquier modelo la interpretación de A_1^2 se comporta como $=$ en otro sentido. Cosas iguales pueden sustituirse una por otra.

Definición 5.3

Los axiomas ($E7$), ($E8$) y ($E9$) se llaman *axiomas de la igualdad.* Toda extensión de $K_{\mathscr{L}}$ que incluya entre sus axiomas a ($E7$) y a todos los casos particulares apropiados de ($E8$) y ($E9$) se dice que es un *sistema de primer orden con igualdad.*

Proposición 5.4

Sea S un sistema de primer orden con igualdad. Entonces las siguientes *fbfs* son teoremas de S:

(i) $(\forall x_1)A_1^2(x_1, x_1)$,

(ii) $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2)\rightarrow A_1^2(x_2, x_1))$,

(iii) $(\forall x_1)(\forall x_2)(\forall x_3)(A_1^2(x_1, x_2)\rightarrow(A_1^2(x_2, x_3)\rightarrow A_1^2(x_1, x_3)))$.

Demostración: (i) Inmediato por Generalización, a partir de ($E7$).
(ii) Demos una demostración en S.

(1) $A_1^2(x_1, x_2)\rightarrow(A_1^2(x_1, x_1)\rightarrow A_1^2(x_2, x_1))$ ($E9$)

(2) $(A_1^2(x_1, x_2)\rightarrow(A_1^2(x_1, x_1)\rightarrow A_1^2(x_2, x_1)))\rightarrow((A_1^2(x_1, x_2)\rightarrow A_1^2(x_1, x_1))\rightarrow(A_1^2(x_1, x_2)\rightarrow A_1^2(x_2, x_1)))$ ($K2$)

(3) $(A_1^2(x_1, x_2)\rightarrow A_1^2(x_1, x_1))\rightarrow(A_1^2(x_1, x_2)\rightarrow A_1^2(x_2, x_1))$ (1), (2), MP

(4) $(A_1^2(x_1, x_1)\rightarrow(A_1^2(x_1, x_2)\rightarrow A_1^2(x_1, x_1)))$ ($K1$)

(5) $A_1^2(x_1, x_1)$ ($E7$)

(6) $(A_1^2(x_1, x_2)\rightarrow A_1^2(x_1, x_1))$ (4), (5), MP

(7) $(A_1^2(x_1, x_2)\rightarrow A_1^2(x_2, x_1))$ (3), (6), MP

(8) $(\forall x_1)(\forall x_2)(A_1^2(x_1, x_2)\rightarrow A_1^2(x_2, x_1))$ (7), Generalización

(iii) De nuevo, demos una demostración en S:

(1) $(A_1^2(x_2, x_1)\rightarrow(A_1^2(x_2, x_3)\rightarrow A_1^2(x_1, x_3)))$ ($E9$)

(2) $(A_1^2(x_1, x_2)\rightarrow A_1^2(x_2, x_1))$ (ii) anterior

(3) $(A_1^2(x_1, x_2)\rightarrow(A_1^2(x_2, x_3)\rightarrow A_1^2(x_1, x_3)))$ (1), (2), HS

(4) $(\forall x_1)(\forall x_2)(\forall x_3)(A_1^2(x_1, x_2)\rightarrow(A_1^2(x_2, x_3)\rightarrow A_1^2(x_1, x_3)))$ (3), Generalización

▷Así pues, como (i), (ii) e (iii) de la proposición anterior han de ser verdaderas en todo modelo de S, el símbolo A_1^2 se interpretará en cualquier modelo mediante una relación reflexiva, simétrica y transitiva, es decir, una relación de equivalencia. Ahora bien, $=$ es la interpretación prevista para A_1^2. En una interpretación arbitraria, los axiomas muy bien pudieran ser falsos, con lo que A_1^2 podría interpretarse mediante cualquier relación binaria; pero en un modelo de S hemos visto que los axiomas tienen que ser verdaderos y A_1^2 deberá interpretarse como una relación de equivalencia. No obstante, los axiomas ($E7$), ($E8$) y ($E9$) no garantizan que en todo modelo de S la interpretación de A_1^2 sea verdaderamente $=$.

Ejemplo 5.5

Considérese el lenguaje de primer orden $\mathscr{L}$ con variables $x_1, x_2, \ldots$, la letra de función f_1^2 y la letra de predicado A_1^2. Defínase una interpretación I como sigue: D_I es el conjunto $\mathbb{Z}$ de los enteros, $f_1^2(x, y)$ es $x+y$, y $A_1^2(x, y)$ se verifica si y sólo si $x \equiv y \pmod 2$, para $x, y \in \mathbb{Z}$. Los axiomas de la igualdad son verdaderos en esta interpretación.

Para ($E7$), la interpretación es $x \equiv x \pmod 2$ que es verdad.

Para ($E8$), considérese el caso particular

$$A_1^2(x_1, x_2) \rightarrow A_1^2(f_1^2(x_1, x_3), f_1^2(x_2, x_3))$$

Esto se interpreta como:

$$\text{si } x \equiv y \pmod 2 \text{ entonces } x+z \equiv y+z \pmod 2$$

que es verdad. La comprobación de ($E8$) en toda su generalidad se deja como ejercicio.

Para ($E9$), solamente hay dos casos que comprobar, pues $\mathscr{L}$ solamente contiene una letra de predicado. Los dos casos son:

$$(A_1^2(t, u) \rightarrow (A_1^2(t, v) \rightarrow A_1^2(u, v)))$$
$$(A_1^2(t, u) \rightarrow (A_1^2(v, t) \rightarrow A_1^2(v, u)))$$

Las respectivas interpretaciones son:

si $x \equiv y \pmod 2$ entonces $x \equiv z \pmod 2$ implica $y \equiv z \pmod 2$

y

si $x \equiv y \pmod 2$ entonces $z \equiv x \pmod 2$ implica $z \equiv y \pmod 2$, que son verdaderas.

▷Este ejemplo muestra que en un modelo de ($E7$), ($E8$) y ($E9$) el símbolo A_1^2 no necesita ser interpretado en todos los casos como $=$. No obstante, la proposición siguiente arregla la situación.

Proposición 5.6

Si S es un sistema de primer orden con igualdad y consistente, entonces S posee un modelo en el cual la interpretación de A_1^2 es $=$.

Demostración: Por la Proposición 4.42, si S es consistente, entonces S tiene un modelo; llamémosle M. $\bar{A}_1^2$ es una relación de equivalencia sobre D_M, debido a la Proposición 5.4. Denotemos por $[x]$ a la clase de equivalencia que contiene a x. Definamos ahora una nueva interpretación M^* como sigue. El dominio de M^* es $\{[x] : x \in D_M\}$, a_i se interpreta como $[\bar{a}_i]$, para todo i, f_i^n se interpreta como $\hat{f}_i^n$, siendo, para $y_1, \ldots, y_n \in D_M$

$$\hat{f}_i^n([y_1], \ldots, [y_n]) = [\bar{f}_i^n(y_1, \ldots, y_n)],$$

y A_i^n se interpreta como $\hat{A}_i^n$, teniéndose que para $y_1, \ldots, y_n \in D_M$ $\hat{A}_i^n([y_1], \ldots, [y_n])$ se verifica si y sólo si se verifica $\bar{A}_i^n(y_1, \ldots, y_n)$ siendo $\bar{a}_i$, $\bar{f}_i^n$, $\bar{A}_i^n$ las interpretaciones de los símbolos de $\mathscr{L}$ en M.

Es tarea pesada, pero no difícil, el demostrar que todas éstas son buenas definiciones y que M^* es un modelo de S. Sea por ejemplo f una letra de función de un argumento de $\mathscr{L}$ y sea $\bar{f}$ su interpretación en M. Supongamos que a y b pertenecen a D_M y que $[a] = [b]$. Tenemos que demostrar que $[\bar{f}(a)] = [\bar{f}(b)]$. Ahora bien,

$$\vdash_S (A_1^2(x_1, x_2) \rightarrow A_1^2(f(x_1), f(x_2))) \qquad (E8)$$

Así pues, $(A_1^2(x_1, x_2) \rightarrow A_1^2(f(x_1), f(x_2)))$ es verdadera en M, ya que M es un modelo, y así $A_1^2(a, b)$ implica $\bar{A}_1^2(\bar{f}(a), \bar{f}(b))$, es decir, $[a] = [b]$ implica $[f(a)] = [f(b)]$.

Además, la interpretación de $\bar{A}_1^2$ en M^* es $=$, ya que $\hat{A}_1^2([x], [y])$ se verifica si y sólo si se verifica $\bar{A}_1^2(x, y)$, es decir, si y sólo si $[x] = [y]$.

▷ Esta demostración puede ilustrarse muy bien con ayuda de nuestro último ejemplo, en el que indicamos un modelo donde A_1^2 no se interpretaba como $=$. En dicho ejemplo teníamos $\bar{A}_1^2(x, y)$ si y sólo si $x \equiv y$ (mod 2) (x e y enteros). Definamos un nuevo modelo de dominio $\{[0], [1]\}$ en el que f_1^2 y A_1^2 se interpretan como $\hat{f}_1^2$ y $\hat{A}_1^2$, dados por

$$\hat{f}_1^2([x], [y]) = [\bar{f}_1^2(x, y)] = [x + y],$$

$\hat{A}_1^2([x], [y])$ se verifica si y sólo si se verifica $\bar{A}_1^2(x, y)$

es decir, si y sólo si $x \equiv y$ (mod 2)
es decir, si y sólo si $[x] = [y]$.

Definición 5.7

Sea S un sistema de primer orden con igualdad. Un modelo *normal* de S es un modelo en el que A_1^2 se interpreta como $=$.

En lo que sigue nos ocuparemos casi siempre de modelos normales, ya que ellos representan la situación matemática prevista, en lo referente a la interpretación de A_1^2.

Nota: Por supuesto, el que hayamos escogido A_1^2 para representar la igualdad no tiene importancia. Podríamos haber escogido del mismo modo A_{17}^2, en cuyo caso en los axiomas (*E*7), (*E*8) y (*E*9) habría aparecido este símbolo de predicado en lugar de A_1^2.

▷Durante el resto de este capítulo nos ocuparemos de sistemas de primer orden con igualdad en los que A_1^2 representará la igualdad. La demostración de la Proposición 5.4 muestra lo repetitivo que puede resultar el escribir nuestras demostraciones; aliviaremos esto un poco introduciendo el símbolo $=$ en nuestro lenguaje en lugar de A_1^2.

Notación: Escribiremos $t_1 = t_2$ en lugar de $A_1^2(t_1, t_2)$, siendo t_1 y t_2 términos de $\mathscr{L}$. Los axiomas (*E*7), (*E*8) y (*E*9) pueden escribirse ahora de forma simplificada, y de un modo que hace ver mucho más claramente su significado.

(*E*7′) $x_1 = x_1$

(*E*8′) $(t_k = u \to (f_i^n(t_1, \ldots, t_k, \ldots, t_n) = f_i^n(t_1, \ldots, n, t_n)))$
$t_1, \ldots, t_n, u, f_i^n$ como en (*E*8)

(*E*9′) $(t_k = u \to (A_i^n(t_1, \ldots, t_k, \ldots, t_n) \to A_i^n(t_1, \ldots, u, \ldots, t_n)))$,
$t_1, \ldots, t_n, u, A_i^n$ como en (*E*9).

El símbolo $=$ no es el único que hemos introducido en el lenguaje formal, añadiéndolo al alfabeto de símbolos original. Por ejemplo, usamos $(\exists x_i)$ como abreviatura de $\sim(\forall x_i)\sim$, y usamos $(\mathscr{A} \leftrightarrow \mathscr{B})$ como abreviatura de $\sim((\mathscr{A} \to \mathscr{B}) \to \sim(\mathscr{B} \to \mathscr{A}))$. A veces resulta conveniente escribir $(\mathscr{A} \vee \mathscr{B})$ como abreviatura de $(\sim\mathscr{A} \to \mathscr{B})$, y $(\mathscr{A} \wedge \mathscr{B})$ como abreviatura de $\sim(\mathscr{A} \to \sim\mathscr{B})$. Ello se corresponde con nuestras ideas intuitivas del Capítulo 1, y está claro que el uso de estos nuevos símbolos no extiende en ningún sentido nuestro sistema formal. Es una cuestión de conveniencia, para evitar tediosas repeticiones de símbolos. En los diferentes contextos que estamos a punto de describir es posible, y a veces deseable, extender esta práctica introduciendo todavía más *símbolos definidos*. En particular, hay uno muy útil que se aplica a cualquier sistema de primer orden con igualdad. Se trata del símbolo correspondiente a «existe un único ... tal que».

Notación: $(\exists_1 x_i)\ \mathscr{A}(x_i)$ es una abreviatura de la fórmula

$$(\exists x_i)(\mathscr{A}(x_i) \wedge (\forall x_j)(\mathscr{A}(x_j) \to x_i = x_j)).$$

Ejercicios

1 En el Ejemplo 5.5, dese una demostración completa de que cualquier caso particular del esquema de axioma (*E*8) es verdadero en la interpretación *I*.

2 Sea *S* un sistema de primer orden con igualdad, y supongamos que la *fbf* cerrada $\mathscr{A}$ es verdadera en todos los modelos normales de *S*. Demuéstrese que $\mathscr{A}$ es verdadera en todos los modelos de *S*.

3 Sea $\mathscr{A}(x_1)$ una *fbf.* de $\mathscr{L}$ en la que x_1 aparece libre; supongamos que x_2 está libre para x_1 en $\mathscr{A}(x_i)$, y sea $\mathscr{A}(x_2)$ el resultado de sustituir *una* de las intervenciones libres de x_1 en $\mathscr{A}(x_1)$ por x_2. (Nótese que esto difiere de la práctica denotacional usual.) Demuéstrese que la *fbf*

$$(x_1 = x_2 \rightarrow (\mathscr{A}(x_1) \rightarrow \mathscr{A}(x_2)))$$

es un teorema de cualquier extensión de *K* en la que (*E*7′), (*E*8′) y (*E*9′) sean axiomas. Dedúzcase el mismo resultado para el caso en que $\mathscr{A}(x_2)$ se obtenga sustituyendo varias intervenciones libres de x_1 por x_2.

4 En la demostración de la Proposición 5.6, demuéstrese que la definición de $\hat{A}_i^n$ está bien hecha, es decir, que si $y_1, \ldots, y_n \in D_M$, $z_1, \ldots, z_n \in D_M$ y $[y_i] = [z_i]$ $(1 \leqslant i \leqslant n)$ entonces $A_i^n(y_1, \ldots, y_n)$ se verifica si y sólo si se verifica $\bar{A}_i^n(z_1, \ldots, z_n)$.

5 Describir el modo de expresar «existen justamente dos ... tales que» en una *fbf* de un sistema de primer orden con igualdad.

6 Sea $\mathscr{A}$ una *fbf.* de $\mathscr{L}$ en la cual los términos $t_1, \ldots, t_n$ intervienen «libremente» en el sentido de que cualquier intervención de una variable en uno de estos términos es libre en $\mathscr{A}$. Sea *S* una extensión de $K_{\mathscr{L}}$ que incluye los axiomas (*E*7′), (*E*8′) y (*E*9′). Demuéstrese que para todo término *u* que no contenga ninguna variable ligada en $\mathscr{A}$,

$$\vdash_S ((t_k = u \rightarrow (\mathscr{A}(t_1, \ldots, t_k, \ldots, t_n) \rightarrow \mathscr{A}(t_1, \ldots, u, \ldots, t_n)))$$

5.3 La teoría de grupos

La teoría de grupos es quizá la rama más familiar de las matemáticas que está basada explícitamente en un conjunto de axiomas sencillo. Tomemos, pues, este «contexto matemático» para ilustrar el modo en que los sistemas matemáticos surgen como extensiones de $K_{\mathscr{L}}$.

Primeramente hemos de describir un lenguaje de primer orden $\mathscr{L}$ adecuado; sea, pues, $\mathscr{L}_G$ el lenguaje de primer orden cuyo alfabeto de símbolos es el siguiente:

variable $x_1, x_2, \ldots$
constante indivisual a_1 (identidad)
símbolos de función f_1^1, f_1^2 (inverso, producto)
símbolo de predicado =
signos de puntuación (,),,
símbolos lógicos $\forall$, $\sim$, $\rightarrow$

Definamos ahora $\mathscr{G}$ como aquella extensión de $K_{\mathscr{S}_G}$ cuyos axiomas propios son (*E*7), todos los casos particulares apropiados de (*E*8) y (*E*9), y los siguientes:

(*G*1) $f_1^2(f_1^2(x_1, x_2), x_3) = f_1^2(x_1, f_1^2(x_2, x_3))$ (ley asociativa)

(*G*2) $f_1^2(a_1, x_1) = x_1$ (identidad por la izquierda)

(*G*3) $f_1^2(f_1^1(x_1), x_1) = a_1$ (inverso por la izquierda)

Como antes, no importa si las variables libres de los axiomas se cuantifican universalmente o no. Los cierres universales de estos axiomas formarían un conjunto de axiomas equivalente.

(*G*1), (*G*2) y (*G*3) no son más que traducción de los axiomas de grupo usuales. Normalmente (*G*2) y (*G*3) se enuncian en la forma «existe una identidad por la izquierda» y «para todo elemento existe un inverso por la izquierda». Nuestros axiomas no afirman explícitamente existencia. Simplemente enuncian que a_1 y $f_1^1(x_1)$, cuando se interpretan en un modelo, deben tener las propiedades adecuadas. No es necesario afirmar existencia, ya que en todo modelo de este sistema habrá interpretaciones de a_1 y de f_1^1, y con ello la identidad y el inverso existirán automáticamente. Análogamente, el axioma de grupo que afirma el carácter cerrado bajo la operación del grupo es innecesario aquí, porque la interpretación de f_1^2 en un modelo es necesariamente una función de dos argumentos con valores en el dominio del modelo.

Dado un sistema así de teoría de grupos, podemos convertir cualquier demostración standard, tomada de un texto de álgebra, de un resultado referente a elementos de grupos, en una demostración formal del sistema. Este procedimiento no tendrá mucha aplicación práctica, puesto que una demostración formal en $\mathscr{G}$ es necesariamente más complicada, y el gran número de pasos puramente manipulativos oscurecería de las ideas intuitivas implicadas, como muestra el siguiente ejemplo.

Ejemplo 5.8)

En todo grupo G cuyo elemento identidad sea e, $e(ee) = e$. En correspondencia con esto, demos una demostración formal en el sistema $\mathscr{G}$ de la *fbf*.

$$f_1^2(a_1, f_1^2(a_1, a_1)) = a_1$$

(1)	$f_1^2(a_1, x_1) = x_1$	(*G*2)
(2)	$(\forall x_1)(f_1^2(a_1, x_1) = x_1)$	(1), Generalización
(3)	$(\forall x_1)(f_1^2(a_1, x_1) = x_1) \rightarrow (f_1^2(a_1, a_1) = a_1)$	(*K*5)
(4)	$f_1^2(a_1, a_1) = a_1$	(2), (3), *MP*
(5)	$(\forall x_1)(f_1^2(a_1, x_1) = x_1) \rightarrow (f_1^2(a_1, f_1^2(a_1, a_1)) = f_1^2(a_1, a_1))$	(*K*5)

(6) $f_1^2(a_1, f_1^2(a_1, a_1)) = f_1^2(a_1, a_1)$ (2), (5), *MP*

(7) $(f_1^2(a_1, a_1) = a_1) \rightarrow (f_1^2(a_1, f_1^2(a_1, a_1))$
$= f_1^2(a_1, a_1) \rightarrow f_1^2(a_1, a_1)) = a_1)$ (*E*9)

(8) $(f_1^2(a_1, f_1^2(a_1, a_1)) = f_1^2(a_1, a_1)$
$\rightarrow f_1^2(a_1, f_1^2(a_1, a_1)) = a_1)$ (4), (7), *MP*

(9) $f_1^2(a_1, f_1^2(a_1, a_1)) = a_1$ (6), (8), *MP*

En comparación con esto, una demostración standard de que $e(ee) = e$ para todo grupo es una trivialidad. Resultados más complicados se reflejan en demostraciones formales en $\mathscr{G}$ todavía más complicadas. No vale mucho la pena exhibir ejemplos particulares, pero se obtendrá algo más de idea de las complicaciones que aparecen tratando de demostrar en $\mathscr{G}$ la *fbf*

$$f_1^2(x_1, a_1) = x_1,$$

que corresponde a la propiedad de los grupos de que la identidad por la izquierda es también la identidad por la derecha.

▷ Debería estar claro que todo grupo G es un modelo del sistema $\mathscr{G}$, suponiendo que a_1 se interprete como el elemento identidad de G, f_1^1 como la operación inversa, f_1^2 como la operación del grupo y $=$ como la igualdad. No obstante, hay otros modelos, como veremos.

Ejemplo 5.9

Constrúyase una interpretación I del sistema $\mathscr{G}$ como sigue. Sea D_I el conjunto $\mathbb{Z}$ de los enteros; interpretemos a_1 como 0; sea

$$\bar{f}_1^1(x) = -x \text{ para } x \in \mathbb{Z},$$

y

$$\bar{f}_1^2(x, y) = x + y \text{ para } x, y \in \mathbb{Z},$$

e interpretemos $=$ como una congruencia (mod m), siendo m un cierto entero positivo fijo. (Aunque estamos usando $=$ como un símbolo de $\mathscr{L}_G$, como vimos más arriba, no es necesario interpretarlo siempre como la verdadera igualdad). I es un modelo de $\mathscr{G}$. Para comprobarlo hemos de demostrar que todo axioma de $\mathscr{G}$ es verdadero en I. El que $(K1)-(K6)$ son verdaderos no requiere verificación, ya que son lógicamente válidos. El que $(E7)$, $(E8)$ y $(E9)$ son verdaderos se comprueba como en el Ejemplo 5.5. Veamos más de cerca lo que ocurre con $(G1)$, $(G2)$ y $(G3)$.

$(G1)$ se interpreta como

$$(x + y) + z \equiv x + (y + z) \pmod{m}$$

($G2$) se interpreta como

$$0 + x \equiv x \pmod{m}.$$

($G3$) se interpreta como

$$-x + x \equiv 0 \pmod{m}.$$

Todos éstos son enunciados verdaderos para todo x, y, $z \in \mathbb{Z}$. Así pues, I es un modelo de $\mathscr{G}$. No obstante, I no es un grupo; de hecho, interviene en él la relación de congruencia, que es extraña. No obstante, el lector que tenga alguna experiencia en teoría de grupos o de números se dará cuenta de que en el fondo hay un grupo esperando ser descubierto. A partir del modelo I podemos construir un modelo normal I^* siguiendo el procedimiento de la Proposición 5.6. El dominio de I^* es el conjunto de clases de congruencia de enteros (mod m), a_1 se interpreta como 0_m (la clase que contiene al 0), f_1^2 se interpreta como $+$ (que está bien definida sobre clases de congruencia), f_1^1 se interpreta como la función «inverso aditivo» (también bien definida) e $=$ se interpreta como la igualdad. I^* es un modelo normal y es un grupo.

▷En general, todo grupo es un modelo normal del sistema formal de teoría de grupos, y recíprocamente, todo modelo normal del sistema es un grupo. Así pues, para que el sistema cobre sentido matemático hemos de restringir nuestra atención a modelos normales. Quizá sea desafortunado, pero es imposible dar axiomas de la igualdad que fuercen a la interpretación a ser la verdadera igualdad. Siempre será posible construir un modelo en el que $=$ se interprete mediante alguna otra relación de equivalencia.

La razón de que hayamos construido este sistema formal de teoría de grupos no es el proporcionar ninguna simplificación o nuevo método para obtener resultados acerca de grupos y elementos de grupos. Como hemos visto, los métodos de demostración de que se dispone en $\mathscr{G}$ son tan engorrosos que carecen de utilidad para este propósito. Lo que hemos ganado al describir el sistema $\mathscr{G}$ es que hemos precisado y explicitado todas las hipótesis y procedimientos que los matemáticos usan en el contexto de la teoría de grupos, incluyendo tanto las hipótesis y procedimientos lógicos como los matemáticos. De esta manera hemos clarificado esta parte de las matemáticas.

Hemos tratado en detalle los grupos, y puede darse un tratamiento similar para otros sistemas algebraicos abstractos, como por ejemplo, los anillos, los cuerpos, los espacios vectoriales, los retículos, las álgebras de Boole, etc. Cada uno de estos tipos de sistema se sabe que puede caracterizarse mediante un conjunto finito de axiomas, y éstos pueden trasladarse fácilmente a un lenguaje formal apropiado. De he-

cho, cualquier área de matemáticas que esté caracterizada por un conjunto de axiomas puede tratarse de modo similar. Por ejemplo, la geometría euclídea puede basarse en un sistema de axiomas bastante extenso y complejo, y el correspondiente sistema formal tendría que contener letras de predicado cuya interpretación prevista fuese «es un punto», «es una recta», «corta», etc. También puede describirse un sistema de axiomas para los números reales, mediante los axiomas de cuerpo ordenado completo.

Hay dos áreas de matemáticas que son particularmente importantes cuando se tratan de esta manera: La aritmética y la teoría de conjuntos. Cada una de ellas requeriría un libro entero para darle un tratamiento completo, pero solamente vamos a tratar de explicar por qué razón ocupan una posición especial. Solamente dentro del marco de un sistema formal explícito es posible clarificar las cuestiones de consistencia, o de relaciones entre diferentes hipótesis, o de posición y uso de hipótesis fundamentales. La teoría de conjuntos sirve de fundamento a todas las matemáticas, así que su base lógica es de importancia decisiva. La aritmética es un fragmento elemental de las matemáticas, y su importancia radica en los métodos utilizados para demostrar que la búsqueda de un sistema formal que permita comprobar la veracidad de cualquier proposición matemática por fuerza ha de ser infructuosa. Cualquier sistema matemático en el que pueda efectuarse la aritmética ordinaria no puede ser un sistema universal de este estilo, puesto que el conjunto de teoremas de toda extensión consistente de la aritmética (en un sentido que se precisará) omite al menos una proposición verdadera. Algunos sistemas que no son extensiones de la aritmética, por ejemplo, la teoría de grupos) no tienen esta propiedad. No obstante, un sistema que incluya el análisis matemático o esté previsto para comprender la totalidad de las matemáticas ciertamente incluirá la aritmética, y sufrirá por tanto de este defecto. Estas materias se discutirán con cierto detalle en el Capítulo 6.

Ejercicios

7 Descríbase un sistema de primer orden $\mathscr{G}'$ de teoría de grupos, usando un lenguaje formal sin constantes individuales. Hágase lo mismo usando un lenguaje formal que contenga a la constante individual a_1, pero que no contenga símbolos de función.

8 Un semigrupo es un conjunto sobre el que está definida una operación binaria asociativa. Descríbase un sistema de primer orden $\mathscr{S}$ de teoría de semigrupos, de modo que el sistema $\mathscr{G}'$ del Ejercicio 7 sea una extensión de $\mathscr{S}$.

9 ¿Cuál es el efecto producido en los modelos del sistema $\mathscr{G}'$ (del Ejercicio 7) si se altera el sistema incluyendo en el lenguaje una sola constante individual a_1 (pero no axiomas adicionales)? ¿Cuál es el efecto de incluir en el lenguaje la sucesión completa $a_1, a_2, \ldots$ de constantes individuales?

10 Descríbase un sistema de primer orden cuyos modelos normales sean todos los grupos *infinitos*. ¿Es posible que un sistema de primer orden tenga como modelos normales a todos los grupos *finitos*?

11 Descríbase en detalle un sistema de primer orden de teoría de anillos, es decir, enumérese la lista de símbolos correspondiente a un lenguaje de primer orden apropiado y escríbase un conjunto de axiomas y esquemas de axiomas. Descríbase un modelo de este sistema que no sea un anillo.

12 Sea $\mathscr{F}$ un sistema de primer orden de teoría de cuerpos. Los modelos normales de este sistema son cuerpos, cuya característica puede ser cero o cualquier número primo p. Demuéstrese que si una *fbf.* cerrada $\mathscr{A}$ del lenguaje $\mathscr{F}$ es verdadera en todos los cuerpos de característica cero, entonces existe un número entero positivo n tal que $\mathscr{A}$ es verdadera en todo cuerpo de característica p, siendo $p > n$.

13 Sea $\mathscr{F}$ como se ha descrito en el Ejercicio 12 y sea $\mathscr{A}$ una *fbf.* tal que para todo p mayor que un cierto n existe un cuerpo de característica p en el que $\mathscr{A}$ es verdadera. Demuéstrese que existe un cuerpo de característica cero en el que $\mathscr{A}$ es verdadera.

5.4 Aritmética de primer orden

Vamos a desarrollar las ideas involucradas en la interpretación aritmética N que se introdujo en el Capítulo 3. Tomamos el lenguaje $\mathscr{L}_N$ de modo que contenga variables $x_1, x_2, \ldots$, la constante individual a_1 (para el 0), las letras de función f_1^1, f_1^2, f_2^2 (sucesor, suma y producto) y el símbolo de predicado $=$, así como los signos de puntuación, las conectivas y el cuantificador. Denotaremos por $\mathscr{N}$ al sistema de primer orden obtenido como extensión de $K_{\mathscr{L}_N}$ añadiendo como axiomas adicionales (*E*7), todos los casos particulares apropiados de (*E*8) y (*E*9) y los siguientes seis axiomas más un esquema de axioma.

$(N1)$ $(\forall x_1) \sim (f_1^1(x_1) = a_1)$.

$(N2)$ $(\forall x_1)(\forall x_2)(f_1^1(x_1) = f_1^1(x_2) \rightarrow x_1 = x_2)$.

$(N3)$ $(\forall x_1)(f_1^2(x_1, a_1) = x_1)$.

$(N4)$ $(\forall x_1)(\forall x_2)(f_1^2(x_1, f_1^1(x_2)) = f_1^1(f_1^2(x_1, x_2)))$.

$(N5)$ $(\forall x_1)(f_2^2(x_1, a_1) = a_1)$.

$(N6)$ $(\forall x_1)(\forall x_2)(f_2^2(x_1, f_1^1(x_2)) = f_1^2(f_2^2(x_1, x_2), x_1))$.

$(N7)$ $\mathscr{A}(a_1) \rightarrow ((\forall x_1)(\mathscr{A}(x_1) \rightarrow \mathscr{A}(f_1^1(x_1))) \rightarrow (\forall x_1)\mathscr{A}(x_1))$,

para cada *fbf* $\mathscr{A}(x_1)$ de $\mathscr{L}_N$ en la que aparezca libre x_1.

Notación: De momento no podemos saber si, por ejemplo, f_1^2 ha de ser interpretada forzosamente en todo modelo normal como la adición (o como una función con las mismas propiedades que la función suma) pero el sistema $\mathscr{N}$ se hará mucho más claro y los axiomas anteriores mucho más fáciles de entender si modificamos $\mathscr{L}_N$ inmediatamente

usando los símbolos $+$, $\times$ y $'$ en lugar de f_1^2, f_2^2 y f_1^1, respectivamente. Para ser más explícitos, escribiremos

$$t_1 + t_2 \text{ en vez de } f_1^2(t_1, t_2)$$
$$t_1 \times t_2 \text{ en vez de } f_2^2(t_1, t_2)$$

y

$$t' \text{ en vez de } f_1^1(t),$$

siendo t_1, t_2 y t términos cualesquiera. Usaremos asimismo el símbolo 0 en lugar de a_1. Una vez más debemos hacer énfasis en los peligros que lleva consigo el hacer esto. Habiéndolo hecho no debemos suponer que estos nuevos símbolos se interpretan siempre necesariamente como las funciones u objetos que normalmente representan.

Usando estos símbolos, los axiomas $(N1)-(N7)$ pueden reescribirse como sigue:

$(N1^*)$ $(\forall x_1)\sim(x_1' = 0)$.
$(N2^*)$ $(\forall x_1)(\forall x_2)(x_1' = x_2' \rightarrow x_1 = x_2)$.
$(N3^*)$ $(\forall x_1)(x_1 + 0 = x_1)$.
$(N4^*)$ $(\forall x_1)(\forall x_2)(x_1 + x_2' = (x_1 + x_2)')$.
$(N5^*)$ $(\forall x_1)(x_1 \times 0 = 0)$.
$(N6^*)$ $(\forall x_1)(\forall x_2)(x_1 \times x_2' = (x_1 \times x_2) + x_1)$.
$(N7^*)$ $\mathscr{A}(0) \rightarrow ((\forall x_1)(\mathscr{A}(x_1) \rightarrow \mathscr{A}(x_1')) \rightarrow (\forall x_1)\mathscr{A}(x_1))$,

para toda *fbf* $\mathscr{A}(x_1)$ en la que aparezca libre x_1.

Observaciones 5.10

(*a*) El lector familiarizado con los Postulados de Peano reconocerá $(N1)$, $(N2)$ y $(N7)$. Los Postulados de Peano son un conjunto de axiomas para el sistema de los números naturales que se hicieron explícitos bastante antes de que los sistemas formales se estudiasen como tales. Son:

1. 0 es un número natural.
2. Para todo número natural n, existe otro número natural n'.
3. Para ningún número natural n es n' igual a 0.
4. Para todo par de números naturales m y n, si $m' = n'$ entonces $m = n$.
5. Para todo conjunto A de números naturales que contenga al 0, si $n' \in A$ siempre que $n \in A$, entonces A contiene a todo número natural.

Nótese que los dos primeros postulados no se corresponden con ninguno de los axiomas de nuestro sistema $\mathscr{N}$. Nosotros no los necesita-

mos porque hemos incluido en el lenguaje $\mathscr{L}_N$ símbolos (0 y ', o bien a_1 y f_1^1) que tienen que tener interpretación en todo modelo, de manera que en todo modelo existe un elemento $\bar{a}_1$, y para todo x tiene que existir un elemento $\bar{f}_1^1(x)$.

(*b*) La correspondencia entre (*N*7) y el quinto Postulado de Peano no es exacta. Ambas son versiones del Principio de Inducción Matemática. No obstante, como en $\mathscr{N}$ estamos restringidos al uso del lenguaje de primer orden $\mathscr{L}_N$, el axioma (*N*7) no puede ser tan fuerte como el quinto Postulado de Peano. La razón es que el quinto Postulado de Peano contiene un cuantificador de segundo orden «para todo conjunto A de números naturales», que no puede expresarse en nuestro lenguaje de primer orden. Lo mejor que podemos hacer es usar la noción de *esquema* de axiomas, con lo que de hecho tenemos un cuantificador en «para todo *fbf* $\mathscr{A}(x_1)$ en la que aparezca libre x_1'. Nótese que una tal *fbf* $\mathscr{A}(x_1)$ determina un conjunto en cada interpretación; concretamente, el conjunto de elementos v_1 del dominio de la interpretación que satisfagan $\mathscr{A}(x_1)$. (Más exactamente, el conjunto de todos los elementos v_1 del dominio de la interpretación tal que toda valoración v tal que $v(x_1)=v_1$ satisface $\mathscr{A}(x_1)$.)

Así pues, si pensamos en el contexto de un modelo de $\mathscr{N}$, cada caso particular del esquema de axioma (*N*7) corresponde a la aserción del quinto postulado de Peano para un cierto conjunto particular. No obstante, permanece aún una diferencia esencial. Los casos particulares del esquema de axioma (*N*7) forman un conjunto numerable de *fbf*s. de $\mathscr{L}_N$. El quinto postulado de Peano es un enunciado relativo a conjuntos de números naturales, y la colección de todos éstos es no numerable. Así pues, (*N*7) es una forma mucho más restringida del Principio de Inducción, ya que se refiere solamente a aquella colección numerable de subconjuntos del dominio de un modelo que pueden «representarse» del modo descrito más arriba por medio de *fbf*s de $\mathscr{L}_N$.

(*c*) Los Postulados de Peano no contienen ninguna mención a sumas o productos. Estas funciones pueden definirse en términos de la función sucesor, usando el principio de inducción, pero es conveniente incluir símbolos para ellas en el lenguaje formal. Habiendo hecho esto, (*N*3)–(*N*6) son necesarios para asegurar que en todo modelo las interpretaciones de estos símbolos tengan las propiedades requeridas.

▷ Matemáticamente, hay una diferencia fundamental entre esta situación y la de los grupos. El sistema formal de teoría de grupos permitía muchos modelos normales diferentes, a saber, todos los grupos. El sistema $\mathscr{N}$ de la aritmética se pretende que tenga un solo modelo normal, a saber, el conjunto de los números naturales, puesto que son las propiedades de los números naturales las que esperamos que aparezcan como teoremas del sistema. Mientras que el especialista en teoría de

grupos puede ocuparse de resultados generales que se verifican en todos los grupos, el especialista en teoría de números se ocupa de resultados referentes a un conjunto particular, el conjunto de los números naturales. Es natural por tanto preguntarse si existen otros modelos normales del sistema $\mathcal{N}$, distintos del conjunto de los números naturales. Otra pregunta que surge de manera natural es si el sistema es suficientemente fuerte, en el sentido de tener como teoremas a todas las *fbfs* que nos gustaría que lo fuesen, es decir, todas las *fbfs* que corresponden a enunciados verdaderos acerca de números naturales. Estas dos cuestiones no están desconectadas, como veremos dentro de poco.

Puede ser que algunos lectores están familiarizados con la demostración standard de que los Postulados de Peano determinan unívocamente el conjunto de los números naturales. Sean N y M «modelos» de los Postulados de Peano. Entonces $0 \in N$ y $0 \in M$. Sea A el conjunto de los elementos de N que son elementos de M. Entonces $0 \in A$. Además, si $n \in A$, entonces $n \in N$ y $n \in M$, luego $n' \in N$ y $n' \in M$, luego $n' \in A$. Así pues, por el quinto Postulado de Peano, A consta de todos los números naturales, es decir, $A = N$, y de este modo $N \subseteq M$. Análogamente, $M \subseteq N$ con lo que $N = M$. En esta demostración se hace uso esencial del quinto Postulado de Peano y, como hemos hecho notar más arriba, $(N7)$ no corresponde exactamente a este Postulado. De hecho, la demostración anterior no puede traducirse a una demostración en $\mathcal{N}$. Así pues, aquí no hay esperanza de obtener una respuesta negativa a nuestra primera pregunta acerca de $\mathcal{N}$.

Volvamos ahora a la pregunta: ¿Es $\mathcal{N}$ completo? Es decir, ¿es $\mathscr{A}$ o $(\sim\mathscr{A})$ siempre un teorema de $\mathcal{N}$, para toda *fbf* cerrada $\mathscr{A}$ de $\mathscr{L}_N$? La importancia de esta pregunta puede no ser obvia a primera vista, pero tiene relación con las dos preguntas de más arriba. Si $\mathcal{N}$ no fuese completo, no existiría ningún sistema suficientemente fuerte en el sentido antes explicado, ya que existiría una *fbf* cerrada $\mathscr{A}$ tal que ni $\mathscr{A}$ ni $(\sim\mathscr{A})$ serían teoremas de $\mathcal{N}$. Ahora bien, en toda interpretación, cada *fbf* cerrada es o verdadera o falsa, así que $\mathscr{A}$ es o verdadera o falsa en la interpretación N; en el segundo caso, $(\sim\mathscr{A})$ será verdadera. Ahora bien, la interpretación de $\mathscr{A}$ en $\mathcal{N}$ es un enunciado acerca de números naturales y, desde el punto de vista intuitivo, o $\mathscr{A}$ o $(\sim\mathscr{A})$ tendrán una interpretación que será un enunciado verdadero acerca de números naturales. Pero ni $\mathscr{A}$ ni $(\sim\mathscr{A})$ son teoremas de $\mathcal{N}$. Así pues, si $\mathcal{N}$ no fuese completo habría un enunciado verdadero acerca de números naturales cuya correspondiente *fbf* en $\mathcal{N}$ no sería un teorema de $\mathcal{N}$. Sería deseable, y ello era parte del ánimo con que originalmente se construyó el sistema $\mathcal{N}$, que todas las *fbf* que son verdaderas en el modelo N fuesen teoremas de $\mathcal{N}$. No obstante, si $\mathcal{N}$ no fuese completo esto no podría ser así.

Además, si existiese *fbf* $\mathscr{A}$ tal que ni $\mathscr{A}$ ni $(\sim\mathscr{A})$ fuesen teoremas de $\mathscr{N}$, entonces (supuesto que el propio $\mathscr{N}$ sea consistente) podríamos obtener, como hicimos al final del Capítulo 4, dos extensiones consistentes distintas de $\mathscr{N}$ añadiendo por un lado $\mathscr{A}$ y por otro $(\sim\mathscr{A})$ como nuevo axioma. Cada una de estas extensiones tendrá un modelo normal (Proposición 5.6) y estos dos modelos son ciertamente modelos de $\mathscr{N}$ que han de ser por fuerza esencialmente diferentes, puesto que $\mathscr{A}$ es verdadera en uno y $(\sim\mathscr{A})$ en el otro. Así pues, si $\mathscr{N}$ no fuese completo existiría necesariamente un modelo normal de $\mathscr{N}$ distinto del previsto.

Que $\mathscr{N}$ no es completo fue uno de los resultados principales obtenidos por Gödel. De hecho, él demostró un resultado mucho más fuerte, del que éste es un caso particular. El Capítulo 6 está consagrado a las ideas y métodos involucrados en la demostración y examina algunas consecuencias. Antes de pasar a ello, vamos a considerar el otro «contexto matemático» importante antes mencionado: la teoría de conjuntos formal.

Ejercicio

14 Podría especificarse un sistema formal $\mathscr{N}'$ para la aritmética del siguiente modo: El lenguaje contiene f_1^1, f_1^2, f_2^2, A_1^1, a_0, a_1, a_2, ..., junto con los signos de puntuación, las conectivas y el cuantificador, como de costumbre. Los axiomas son los mismos de $\mathscr{N}$, con la adición de $f_1^1(a_i)=a_{i+1}$, para todo $i>0$. Está claro que N es un modelo normal de este sistema, supuesto que a_k se interprete como $k-1$, para todo entero positivo k. (La interpretación de a_0 no tiene importancia).
Considérese ahora el sistema obtenido a partir de $\mathscr{N}'$ incluyendo como axiomas adicionales todas las *fbfs* $\sim(a_0=a_i)$ para $i>0$. Considerando los modelos, demuéstrese que este nuevo sistema es consistente y posee por lo tanto un modelo normal. ¿En qué se diferencia un modelo así de N?

5.5 Teoría de conjuntos formal

Los fundamentos de las matemáticas están asentados hoy en día en la teoría de conjuntos, y desde comienzos de siglo los matemáticos han investigado los supuestos básicos que se han de hacer acerca de los conjuntos (es decir, los axiomas) y los modos en que la totalidad de las matemáticas pueden edificarse sobre estos supuestos. La ventaja de desarrollar una teoría de conjuntos formal radica en que las hipótesis se hacen explícitas, lo cual proporciona una oportunidad de criticarlas y de explorar interdependencias entre ellas. Vamos a describir un sistema de teoría de conjuntos formal. Hay otros, pero el nuestro es uno de los standard, y quizás el más sencillo de describir en términos de los conceptos que ya hemos discutido. El lector que no esté familiarizado con la fundamentación de las matemáticas sobre la base de la

teoría de conjuntos puede que encuentre difíciles los mismos axiomas, pero se les ha incluido aquí para completar la exposición y dar alguna idea de su naturaleza. Lo que sigue no depende de ellos. No disponemos de espacio más que para describir el sistema y apuntar algunas de las maneras en que la teoría de conjuntos se desarrolla a partir de él.

El sistema que vamos a describir se llama ZF. El nombre se deriva de Ernst Zermelo, que fue el primero en formular una colección de axiomas para teoría de conjuntos en 1905, y Abraham Fraenkel, que los modificó en 1920.

El lenguaje de primer orden apropiado para ZF contiene variables, signos de puntuación, conectivas y el cuantificador, como de costumbre, y los símbolos de predicado $=$ y A_2^2 (no hay letras de función ni constantes individuales). A_2^2 quiere representar a $\in$, la relación de pertenencia. De hecho, con la misma advertencia que hicimos en el caso de $\mathscr{L}_N$, consideraremos a $\in$ como un símbolo del lenguaje, que ocupará el lugar de A_2^2, y escribiremos $t_1 \in t_2$ en lugar de $A_2^2(t_1, t_2)$, cualquiera que sean los términos t_1 y t_2. Nótese que la falta de constantes individuales y letras de función significa que los únicos términos son las variables y que las únicas fórmulas atómicas son las de la forma $x_i = x_j$ o $x_i \in x_j$. Esto puede parecer muy restrictivo, pero los axiomas que introduciremos garantizarán que el sistema formal refleje verdaderamente toda la generalidad de la teoría de conjuntos intuitiva, y podremos introducir símbolos definidos correspondientes a las nociones standard de la teoría de conjuntos, tales como el conjunto vacío, la unión, el conjunto potencia, etc.

ZF se define como la extensión de $K_{\mathscr{L}}$ (siendo $\mathscr{L}$ el lenguaje descrito arriba) obtenido incluyendo como axiomas ($E7$), todos los casos particulares de ($E9$) (($E8$) no tiene casos particulares no triviales), y ($ZF1$)-($ZF8$) que se numeran más abajo.

$$(ZF1) \quad (x_1 = x_2 \leftrightarrow (\forall x_3)(x_3 \in x_1 \leftrightarrow x_3 \in x_2))$$

Este es el llamado Axioma de Extensionalidad, y pretende significar que dos conjuntos son iguales si y sólo si tienen los mismos elementos. Nótese que la implicación de izquierda a derecha viene dada ya por ($E9$), pero el significado del axioma es más claro si se incluyen ambas implicaciones.

$$(ZF2) \quad (\exists x_1)(\forall x_2) \sim (x_2 \in x_1)$$

Este es el Axioma del Conjunto Vacío, ya que garantiza la existencia, en la interpretación prevista, de un conjunto sin elementos. Es consecuencia de ($ZF1$) que en todo modelo normal habrá solamente un conjunto así. Podemos pues introducir en el lenguaje el símbolo ϕ para actuar como constante individual, y ($ZF2$) toma la forma de la *fbf.* $(\forall x_2) \sim (x_2 \in \phi)$.

Notación: Introducimos el símbolo $\subseteq$ como abreviatura del modo siguiente:

$$(t_1 \subseteq t_2) \text{ es abreviatura de } (\forall x_1)(x_1 \in t_1 \rightarrow x_1 \in t_2)$$

siendo t_1, t_2 términos cualesquiera.

$(ZF3)$ $(\forall x_1)(\forall x_2)(\exists x_3)(\forall x_4)(x_4 \in x_3 \leftrightarrow (x_4 = x_1 \vee x_4 = x_2))$

Este es el Axioma de Apareamiento. Dados dos conjuntos cualesquiera x e y existe un conjunto z cuyos miembros son x e y. Este es también un axioma que afirma existencia, y es conveniente introducir en el lenguaje los símbolos $\{y\}$ a fin de denotar el objeto cuya existencia afirma el axioma. $\{x_1, x_2\}$ se considerará como un término, y $(ZF3)$ afirma entonces $x_4 \in \{x_1, x_2\} \leftrightarrow (x_4 = x_1 \vee x_4 = x_2)$.

$(ZF4)$ $(\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \leftrightarrow (\exists x_4)(x_4 \in x_1 \wedge x_3 \in x_4))$

Este es el Axioma de la Unión. Dado cualquier conjunto x, existe un conjunto y que tiene como elementos a los elementos de los elementos de x.

Notación: Denotamos por $\cup x_1$ al objeto cuya existencia se afirma en $(ZF4)$. $\cup x_1$ actúa como símbolo de función de un argumento. Podemos entonces introducir $\cup$ poniendo:

$$(t_1 \cup t_2) \text{ es abreviatura de } \cup\{t_1, t_2\}.$$

$(ZF5)$ $(\forall x_1)(\exists x_2)(\forall x_3)(x_3 \in x_2 \leftrightarrow x_3 \subseteq x_1)$

Este es el Axioma del Conjunto Potencia. Dado cualquier conjunto x existe un conjunto y cuyos elementos son todos los subconjuntos de x.

$(ZF6)$ $(\forall x_1)(\exists_1 x_2).\mathscr{A}(x_1, x_2) \rightarrow$

$(\forall x_3)(\exists x_4)(\forall x_5)(x_5 \in x_4 \leftrightarrow (\exists x_6)(x_6 \in x_3 \wedge \mathscr{A}(x_6, x_5)))$

para toda *fbf* $\mathscr{A}(x_1, x_2)$ en la que aparezcan libres x_1 y x_2 (y en la cual podemos suponer sin pérdida de generalidad que no aparecen los cuantificadores $(\forall x_5)$ y $(\forall x_6)$).

Este es el Esquema de Reemplazamiento. Si la *fbf* $\mathscr{A}$ determina una función, entonces para todo conjunto x existe un conjunto y que tiene como elementos todas las imágenes de elementos de x bajo esta función.

$(ZF6)$ $(\exists x_1)(\phi \in x_1 \wedge (\forall x_2)(x_2 \in x_1 \rightarrow x_2 \cup \{x_2\} \in x_1))$

(Nota: $\{x_2\}$ es abreviatura de $\{x_2, x_2\}$ ya definido antes).

Este es el Axioma de Infinitud. Asegura la existencia, en todo modelo, de un conjunto infinito. Si no estuviese incluido entre los axiomas no habría ningún modo de asegurar que el sistema formal es revelante

con respecto a la teoría de conjuntos intuitiva, que incluye conjuntos infinitos.

$$(ZF8)\quad (\forall x_1)(\sim x_1 = \phi \rightarrow (\exists x_2)(x_2 \in x_1 \wedge \sim(\exists x_3)(x_3 \in x_2 \wedge x_3 \in x_1)))$$

Este es el Axioma de Fundamento. Todo conjunto no vacío x contiene un elemento disjunto con x. Este es un axioma técnico que se incluye para evitar anomalías contrarias a la intuición, tales como la posibilidad de que un conjunto sea elemento de sí mismo.

ZF es un sistema formal de teoría de conjuntos. Los axiomas se han escogido de manera que las interpretaciones de los símbolos formales en modelos normales se comporten como lo hacen los conjuntos. Algunos de los axiomas tienen una base intuitiva más fuerte que otros, pero estos ocho han resistido a la prueba del tiempo y parecen representar verdades básicas acerca de los conjuntos.

ZF puede usarse como base del análisis matemático del siguiente modo: Supuesto que sea un sistema consistente, sabemos que existe un modelo normal. Puede demostrarse que en cualquier modelo así hay conjuntos que poseen todas las propiedades usuales de los sistemas numéricos. Los detalles de este punto son tediosos y no podemos tratarlos aquí. Por ejemplo, un modelo del sistema $\mathcal{N}$ de la aritmética puede definirse como un subconjunto de un modelo de ZF del siguiente modo. $\varnothing$ tiene una interpretación en el modelo de ZF, llamémosla $\bar{\varnothing}$. Entonces $\{\bar{\varnothing}\}$ es un elemento diferente del modelo (el conjunto cuyo único elemento es $\bar{\varnothing}$), y $\{\bar{\varnothing}, \{\bar{\varnothing}\}\}$ es otro (este conjunto tiene dos elementos $\bar{\varnothing}$ y $\{\bar{\varnothing}\}$). Este es el principio de un proceso de inducción que genera una sucesión de conjuntos. La regla general es: Para cada x de la sucesión, su sucesor es $x \cup \{x\}$. Puede comprobarse fácilmente que el $(k+1)$-ésimo miembro de esta sucesión tiene k elementos, y es posible *definir* el número natural k como este miembro $(k+1)$-ésimo. Ya hemos visto que las otras operaciones aritméticas pueden definirse en términos de la función sucesor. Los axiomas $(N1)$- ... $(N7)$ son entonces consecuencia de las definiciones y los axiomas de ZF. Nótese que $(ZF7)$ se necesita para asegurar que la colección de todos los elementos de esta sucesión es un elemento de nuestro modelo normal de ZF. De este modo, todo modelo normal de ZF contiene como elemento a un modelo normal de $\mathcal{N}$.

El lector con formación matemática quizá esté familiarizado con el modo en que los sistemas numéricos de enteros, racionales, reales y complejos pueden construirse a partir de los números naturales mediante procedimientos algebraicos. Todos estos procedimientos pueden llevarse a cabo en ZF. Se necesitan muchas verificaciones detalladas, pero el resultado final confirma que todo modelo normal de ZF contiene como elemento a un conjunto que se parece a y se comporta como el de

los números complejos. (Este conjunto, por supuesto, tiene un subconjunto que se parece a y se comporta como el conjunto de los números reales.)

Aparte de la fundamentación del análisis sobre una base axiomática, hubo otros estímulos a finales del siglo pasado y principios de éste para el estudio de la teoría de conjuntos axiomática: El encontrar una justificación intuitiva (si la había) para el uso de ciertos principios en matemáticas. La atención se centró entonces en dos principios particulares: El axioma de elección (del que se conocían varias formulaciones equivalentes) y la hipótesis del continuo. Resulta bastante esclarecedor el investigar algo de la historia de estos principios desde entonces. Algunos matemáticos los han considerado como axiomas adicionales de la teoría de conjuntos, y otros los han considerado como sospechosos desde el punto de vista intuitivo, o incluso como falsedades.

El axioma de elección es:

(AC) Para todo conjunto no vacío x existe un conjunto y que tiene justamente un elemento en común con cada miembro de x.

(Dos de las formulaciones equivalentes más conocidas son: *El lema de Zorn:* Si toda cadena de un conjunto parcialmente ordenado tiene alguna cota superior, entonces el conjunto tiene algún elemento maximal; y el *Principio de Buena Ordenación:* Todo conjunto admite un buen orden.)

La hipótesis del continuo es:

(CH) Todo conjunto infinito de números reales es numerable o tiene el mismo cardinal que el conjunto de todos los números reales. (Dos conjuntos tienen el mismo cardinal si existe una biyección entre ellos.)

Como los matemáticos no estaban de acuerdo acerca de la aceptabilidad de estos dos principios, la pregunta natural que se hizo fue: ¿Son verdaderos? La siguiente pregunta es: Si se trata de demostrar estos principios, ¿sobre qué principios deberían basarse las demostraciones? Zermelo y Fraenkel (y otros) enumeraron los que ellos consideraban fundamentales de la teoría de conjuntos, y el problema pasó a ser: ¿Pueden deducirse (AC) y (CH) como teoremas del sistema ZF de teoría de conjuntos, y en caso negativo, sería consistente el incluir uno o ambos como axiomas adicionales?

Gödel (en 1938) respondió a una de estas preguntas mediante consideraciones técnicas del sistema formal de teoría de conjuntos. (AC) y (CH) son consistentes con ZF. En otras palabras, pueden añadirse como axiomas adicionales sin introducir ninguna contradicción. La idea

es muy simple: Bajo la hipótesis de que ZF sea consistente, Gödel construyó modelos en los que son verderos (AC) y (CH). Así pues, por las Proposiciones 4.41 y 4.42, los sistemas obtenidos añadiendo (AC) o (CH) como axiomas adicionales son ambos consistentes. Incidentalmente, Gödel demostró también que el sistema obtenido añadiendo simultáneamente (AC) y (CH) es también consistente.

Mucho después, Cohen (1963) resolvió el otro problema demostrando que ni (AC) ni (CH) pueden deducirse como teoremas de ZF. De nuevo, la idea es sencilla, aunque la demostración en sí no lo es. Cohen construyó modelos de ZF en los que son ciertas las negaciones de (AC) y (CH). Ahora bien, si (AC) y (CH) fuesen teoremas de ZF serían verdaderos en todo modelo, y una *fbf* y su negación no pueden ser ciertas a la vez en un mismo modelo.

La conclusión de todo esto es que ni (AC) ni $\sim(AC)$ son teoremas de ZF, y que sería consistente incluir cualquiera de ellos como nuevo axioma. Lo mismo ocurre con (CH) y con $\sim(CH)$. La teoría formal de conjuntos ha aclarado los fundamentos, y la aceptación o no aceptación de (AC) y (CH) ha de ser forzosamente decidida por la intuición, o por algún principio matemático no descubierto aún, que pudiese ser aceptado en el futuro como nuevo axioma y confirmarse o refutarse (AC) y (CH). (Incidentalmente, el trabajo de Gödel y Cohen demuestra también que (AC) y (CH) son independientes entre sí; ninguno de ellos es teorema del sistema resultante de añadir el otro a ZF como axioma adicional.)

El estudio de modelos de ZF, de diferentes interpretaciones posibles de $\in$, de la independencia entre axiomas, y de la relación entre la clase de los teoremas de ZF y la clase de los enunciados «verdaderos» de la teoría de conjuntos es un campo fundamental de las matemáticas en el que no entraremos, salvo para hacer las observaciones que siguen a continuación.

Ejercicio

15 ¿Cómo habría que modificar los axiomas del sistema formal de teoría de conjuntos si el lenguaje incluyese los símbolos a_1 (para ϕ), f_1^2 (para $\{\ ,\ \}$) y A_3^2 (para $\subseteq$)? Supongamos el conjunto de los números naturales definido, como en el texto, poniendo $0=\phi$ y $n+1=n\cup\{n\}$, dentro de un modelo de ZF. Demuéstrese que en la interpretación del lenguaje de ZF cuyo dominio es este conjunto y en el cual $\in$ e $=$ se interpretan como la pertenencia y la igualdad verdaderas, los axiomas $(ZF1)$, $(ZF2)$, $(ZF4)$ y $(ZF8)$ son verdaderos, y $(ZF3)$, $(ZF5)$ y $(ZF7)$ son falsos. ¿Es $(ZF6)$ verdadero o falso?

5.6 Consistencia y modelos

Todo sistema de primer orden es consistente si y sólo si tiene un modelo. Es posible argüir entonces que los sistemas matemáticos que hemos descrito son consistentes porque en cada caso hemos estado reflejando en los axiomas las propiedades de un modelo preconcebido. No obstante, el lector observador habrá reparado en una posible circularidad de nuestros argumentos, que puede ejemplificarse mediante la definición de interpretación del Capítulo 3, como un *conjunto* provisto de ciertas operaciones y relaciones. ¿Cómo podemos hablar entonces de modelos de ZF, el sistema formal de teoría de conjuntos, sin caer en una circularidad? La respuesta está en las ideas ya anteriormente mencionadas de una metateoría que incluya las hipótesis necesarias para demostrar resultados referentes a sistemas formales. Cuando tratamos del sistema $\mathcal{N}$, por ejemplo, es posible usar ZF como metateoría, pues ZF «contiene» a $\mathcal{N}$ en un sentido al que ya nos referimos antes. No obstante, al discutir ZF alcanzamos, por así decirlo, el final de la línea. Por su naturaleza, ZF es apropiado para teoría de conjuntos, y con ello para la totalidad de las matemáticas. No obstante, para estudiar ZF requeriríamos métodos matemáticos que no son parte de ZF. La noción de una interpretación de ZF puede definirse solamente en términos de alguna metateoría intuitiva relativa a los conjuntos «reales». Los elementos de un modelo de ZF se han de pensar como conjuntos que interpretan los símbolos de ZF. No obstante, el dominio de un modelo de ZF, aun siendo un conjunto «real», no puede ser un conjunto en el mismo sentido en que lo son los elementos de dicho conjunto, ya que no puede ser la interpretación de un símbolo de ZF.

En estas materias hay ciertas dificultades intuitivas y semánticas, y por esta razón las demostraciones de consistencia por medio de modelos se suelen considerar inadecuadas. El enfoque más respetable es el siguiente: Dados dos sistemas de primer orden S y S^*, podemos tratar de demostrar que puede construirse un modelo para S bajo la hipótesis de que exista un modelo para S^*. Esto proporcionaría una demostración de *consistencia relativa.* Hay una situación en la que esto es casi trivial.

Proposición 5.11

Sea S^* una extensión de S («extensión» en el sentido de la Definición 4.32). Entonces, si S^* es consistente, S lo es también.

Demostración: Supongamos que S^* es consistente pero que S no lo es. Entonces $\vdash_S \mathscr{A}$ y $\vdash_S (\sim\mathscr{A})$, para alguna *fbf* $\mathscr{A}$ de S. Pero $\mathscr{A}$ es también una *fbf* de S^*, y toda demostración en S es también una demostración en S^*, de modo que $\vdash_{S^*} \mathscr{A}$ y $\vdash_{S^*} (\sim\mathscr{A})$, en contradicción con la consistencia de S^*.

▷ Esta es la situación más sencilla que puede presentarse. En los casos

en que S^* no es extensión de S en este sentido, por ejemplo cuando los lenguajes de los dos sistemas son diferentes, la demostración de la consistencia relativa sería más difícil y podría involucrar la construcción de un modelo de S^*. Ya hemos dado una construcción así, si bien esquemáticamente, al demostrar que la consistencia de ZF implica la consistencia de $\mathcal{N}$.

No se sabe si ZF es consistente. La mayoría de los lógicos creen que lo es, pero cualquier intento de demostrar la consistencia tropezaría con dificultades del tipo descrito arriba. Esencialmente, ello requeriría suponer la consistencia de un sistema formal más comprehensivo que ZF. Ciertamente, no se presentarían dificultades análogas a éstas en un intento de demostrar la inconsistencia. Todo lo que haría falta para ello sería un ejemplo de una *fbf* $\mathscr{A}$ tal que $\mathscr{A}$ y $(\sim\mathscr{A})$ fuesen teoremas de ZF. Lo dicho arriba lleva implícito que hasta ahora no se ha encontrado ninguna *fbf* así. Setenta años de búsqueda infructuosa aportan evidencia de que no existen *fbfs* así, pero esto no es en modo alguno concluyente.

Finalmente, notemos un resultado acerca de modelos de ZF que es consecuencia de la Proposición 4.45, y que a primera vista parece contradictorio. ZF es un sistema de primer orden. Bajo la hipótesis de que ZF sea consistente, la Proposición 4.45 afirma que ZF tiene un modelo *numerable*. Ahora bien, intuitivamente existen conjuntos no numerables, de modo que cabe esperar que los modelos de ZF sean no numerables para que puedan contener a tales conjuntos. Esta aparente paradoja se llama Paradoja de Skolem, pero podemos eludir la contradicción directa considerando con cuidado lo que es un modelo, del siguiente modo:

Para ser específicos, el axioma ($ZF5$) se interpreta como: «dado cualquier conjunto x, existe un conjunto que consta de todos los subconjuntos de x». Si x es un conjunto infinito numerable, las reglas de la teoría de conjuntos aseguran que x tiene una cantidad no numerable de subconjuntos. ¿Cómo puede pertenecer el conjunto de todos los subconjuntos de un tal conjunto x a un modelo numerable? Un modelo numerable de ZF consta de conjuntos. Para todo conjunto «real» x que pertenezca al modelo (evidentemente tiene que haber conjuntos «reales» que no pertenezcan al modelo), el axioma ($ZF5$) afirma que todos los subconjuntos de x que pertenecen al modelo forman un conjunto y que pertenece también al modelo. Este conjunto y será numerable cuando se le considere como un conjunto «real», pero será no numerable al considerarlo como elemento del modelo. Un conjunto infinito es no numerable si no existe ninguna biyección entre él y el conjunto de los números naturales. En el modelo no habrá ninguna biyección entre el conjunto de los números naturales e y (todas las posibles biyecciones 'reales' de este tipo faltarán del modelo, del mismo modo que faltan subconjuntos de x).

6
El Teorema de Incompletitud de Gödel

6.1 Introducción

En el Capítulo 5 se han dado ya algunas indicaciones acerca de la importancia del problema de si el sistema $\mathcal{N}$ de la aritmética formal es completo. En este capítulo vamos a describir la demostración de Gödel de que $\mathcal{N}$ no es completo. Se trata de una demostración muy técnica, y de hecho omitimos algunas partes más técnicas, pero existen dos razones para tratarla con algún detalle. La primera es que éste es un resultado fundamental para el estudio de los sistemas formales y de su valor en lo relativo a la fundamentación de las matemáticas, por lo cual es interesante ver qué tipo de demostración se requiere y entender los conceptos subyacentes a ella. La segunda es que la demostración introduce varias nociones nuevas cuya importancia y utilidad rebasa su uso inmediato aquí, siendo uno de los propósitos de este libro el introducir estas nociones. Las más importantes de ellas son las funciones y relaciones recursivas, la numeración de Gödel y la expresabilidad, y éstas se tratan en las subsiguientes secciones de este capítulo tanto por sí mismas como con vistas a su aplicación en la demostración del teorema de Gödel. Las ideas de recursividad se prosiguen en el Capítulo 7; las otras secciones de este capítulo no son prerrequisito para dicha materia. Debido al modo en que este capítulo está estructurado, puede resultar difícil captar la visión de conjunto de la demostración a partir de las últimas secciones, y comenzaremos con un breve esbozo de la estructura de la demostración. El lector que no tenga especial interés por los detalles técnicos puede omitir los detalles de las Secciones 2, 4 y 5 sin perjuicio de lo que sigue.

Gödel demostró la existencia de una *fbf* cerrada $\mathcal{U}$ de $\mathcal{N}$ tal que ni $\mathcal{U}$ ni $(\sim\mathcal{U})$ son teoremas de $\mathcal{N}$. Lo hizo describiendo explícitamente a $\mathcal{U}$ y demostrando que de la suposición de que $\mathcal{U}$ o $(\sim\mathcal{U})$ sea un teorema de $\mathcal{N}$ se sigue una contradicción. La primera idea técnica es la de código. Se indica un método (numeración de Gödel) mediante el cual se

asigna un número de código (entero positivo) a cada *fbf* y a cada sucesión finita de *fbfs*, de tal modo que la *fbf* o sucesión finita de *fbfs* se recupera fácilmente a partir de su número de código. A través de este código, los enunciados referentes a enteros positivos pueden considerarse como enunciados referentes a números de código de expresiones en $\mathcal{N}$, o incluso referentes a las propias expresiones en $\mathcal{N}$. Por ejemplo, consideraremos una relación binaria en D_N que denotaremos por *Dm*, definida así: *Dm*(m, n) se verifica si y sólo si m es el número de código de una demostración en $\mathcal{N}$ de la *fbf*. cuyo número de código es n.

Ahora bien, las *fbfs* de $\mathcal{N}$ con variables libres se interpretan en N como relaciones entre enteros no negativos, de modo que es razonable preguntar: ¿Existe alguna *fbf* de $\mathcal{N}$ que se interprete como la relación *Dm*? Por razones técnicas hacemos una pregunta ligeramente distinta. Observemos primero que en el lenguaje de $\mathcal{N}$ existen términos 0, 0′, 0″, ... correspondientes a (es decir, interpretados en N como) los enteros no negativos 0, 1, 2, ... Denotaremos a estos términos por 0, $0^{(1)}$, $0^{(2)}$, ... Preguntamos entonces: ¿Existe una *fbf* $\mathscr{P}(x_1, x_2)$ de $\mathcal{N}$ con dos variables libres, tal que para todo m, $n \in D_N$, o $\mathscr{P}(0^{(m)}, 0^{(n)})$ o $\sim\mathscr{P}(0^{(m)}, 0^{(n)})$ es un teorema de $\mathcal{N}$, según $D_m(m, n)$ se cumpla en N o no? Si ello es así, se dice que D_m es expresable en $\mathcal{N}$ mediante la *fbf* $\mathscr{P}$.

El siguiente paso es obtener una condición suficiente para que una relación sea expresable en $\mathcal{N}$, y aquí es donde interviene la recursividad. La definición puede verse en la Sección 6.3; aquí nos limitamos a enunciar que si una relación es recursiva, es expresable en $\mathcal{N}$. Es más fácil comprobar la recursividad que la expresabilidad, y es a través de la recursividad como la demostración de Gödel prueba que una relación particular es expresable en $\mathcal{N}$. La relación *Dm* de más arriba es de hecho recursiva, y este hecho se usa en la demostración de que la relación W es recursiva también, estando definida W como sigue: $W(m, n)$ se verifica si m es el número de código de una *fbf* $\mathscr{A}(x_1)$ en la que aparece libre x_1, y n es el número de código de una demostración de la *fbf* $\mathscr{A}(0^{(m)})$. Vale la pena dedicar un poco de esfuerzo a captar el significado de W, ya que introduce una clase de «autorreferencia» que es legítima y crucial para la demostración.

Esta relación W es recursiva y, por lo tanto, expresable en $\mathcal{N}$ mediante una *fbf* $\mathscr{W}$. A partir de esta $\mathscr{W}$, la *fbf*. $\mathscr{U}$ se construye por medio de un procedimiento bastante simple, y $\mathscr{U}$ tiene como interpretación en N: Para todo $n \in D_N$, n no es el número de código de una demostración en $\mathcal{N}$ de la *fbf*. $\mathscr{U}$. Así pues, $\mathscr{U}$ parece involucrar una forma de autorreferencia aún más alarmante, ya que puede considerarse que afirma su propia indemostrabilidad. Las dificultades se evitan distinguiendo cuidadosamente entre las *fbfs* y sus números de código, y entre los términos $0^{(n)}$ y los números que ellos representan. Es bastante

inmediato demostrar que si $\mathscr{U}$ fuese un teorema de $\mathscr{N}$ se deduciría una contradicción, y apenas un poco más difícil el deducir una contradicción supuesto de que $\sim\mathscr{U}$ sea un teorema de $\mathscr{N}$. Por supuesto, se tiene implícitamente la hipótesis de que $\mathscr{N}$ es consistente (pues en otro caso $\mathscr{U}$ y $\sim\mathscr{U}$ serían automáticamente teoremas de $\mathscr{N}$), y, de hecho, para demostrar que $\sim\mathscr{U}$ no es un teorema se requiere una hipótesis acerca de $\mathscr{N}$ ligeramente más fuerte que la consistencia.

Este es, pues, el esbozo de la demostración. En el resto del Capítulo se irá recubriendo el esqueleto, y las consecuencias del resultado se darán en la Sección 6.5. Algunas demostraciones se omiten, y se refiere al lector al libro de Mendelson para la consulta más cuidadosa de los detalles técnicos.

6.2 Expresabilidad

Continuamos aquí el estudio del sistema $\mathscr{N}$ de la aritmética que se ha descrito en el Capítulo 5, y de su modelo previsto N. Uno de los conceptos más importantes que se originan en el estudio de la lógica, el de recursividad, resulta directamente de la relación entre este sistema formal y el modelo N. Las aplicaciones de las funciones recursivas se han desarrollado extensamente en los últimos cuarenta años, pero originalmente surgieron de manera natural a partir de cuestiones referentes a expresabilidad, y éste es el punto del que partiremos.

En anteriores capítulos nos hemos ocupado de los símbolos de sistemas formales y de los modos en que pueden interpretarse. En la presente situación invertiremos este proceso. Partamos del modelo N, cuyo dominio es el conjunto de los números naturales, que seguiremos denotando por D_N. Observemos primeramente que el número 0, la función sucesor, la adición, la multiplicación y la igualdad están representados en el sistema $\mathscr{N}$ de manera obvia, a través de los símbolos de $\mathscr{N}$. Pero consideremos, por ejemplo, el número 5. 5 es un elemento de D_N, pero *no es* un símbolo de $\mathscr{N}$. No obstante, 5 es la interpretación en N de un término particular, a saber $0''''''$, es decir, $f_1^1(f_1^1(f_1^1(f_1^1(f_1^1(a_1)))))$. Todo número natural es la interpretación de un término de $\mathscr{N}$, de manera similar. Tendremos ocasión de utilizar estos términos, y por ello es útil introducir una notación más conveniente que cualquiera de las anteriores, ya que ambas son engorrosas.

Notación: $0^{(n)}$ es una abreviatura de 0 seguido de n primas. Así pues, el *número* $n \in D_N$ es la interpretación en N del *término* $0^{(n)}$. Trivialmente, $0^{(0)}$ representa a la constante individual 0 de $\mathscr{N}$.

Es importante observar que aunque usamos $0^{(n)}$ para designar un término de $\mathscr{N}$, el símbolo n en sí no es un símbolo de $\mathscr{N}$ y la n que

aparece en $0^{(n)}$ no *puede* sustituirse por una variable. Llamaremos a los términos $0^{(n)}$ *términos numerales.*

Proposición 6.1

Sean m, $n \in D_N$.

(i) Si $m \neq n$, entonces $\vdash_{\mathcal{N}} \sim(0^{(m)} = 0^{(n)})$.

(ii) Si $m = n$, entonces $\vdash_{\mathcal{N}} (0^{(m)} = 0^{(n)})$.

Demostración: (i) Supongamos sin restricción de la generalidad que $m < n$. Entonces existe $k > 0$ tal que $n = m + k$. El axioma $(N2^*)$ nos da

$$\vdash_{\mathcal{N}} (0^{(m)} = 0^{(m+k)} \rightarrow 0^{(m-1)} = 0^{(m+k-1)})$$

si $m > 0$, y repetidas aplicaciones junto con el uso de la regla SH, nos dan

$$\vdash_{\mathcal{N}} (0^{(m)} = 0^{(m+k)} \rightarrow 0^{(0)} = 0^{(k)}).$$

(Esto se tiene también trivialmente si $m = 0$.)

Ahora bien, $k > 0$ por hipótesis, luego $k - 1 \in D_N$ y

$$\vdash_{\mathcal{N}} (0^{(k)} = (0^{(k-1)})').$$

(Si esto no está claro piense en ello así:

$$\vdash_{\mathcal{N}} (0''\overset{k}{\ldots}' = (0''\overset{k-1}{\ldots}')').)$$

Así pues, tenemos

$$\vdash_{\mathcal{N}} (0^{(m)} = 0^{(m+k)} \rightarrow 0^{(0)} = (0^{(k-1)})').$$

Haciendo uso de una tautología, obtenemos

$$\vdash_{\mathcal{N}} (\sim(0^{(0)} = (0^{(k-1)})') \rightarrow \sim(0^{(m)} = 0^{(m+k)})).$$

Pero el axioma $(N1^*)$ nos da

$$\vdash_{\mathcal{N}} (\sim(0^{(0)} = (0^{(k-1)})'),$$

con lo cual MP nos lleva a

$$\vdash_{\mathcal{N}} (\sim(0^{(m)} = 0^{(m+k)}) \text{ como queríamos.}$$

(ii) Supongamos que $m = n$. Entonces $0^{(m)}$ y $0^{(n)}$ son idénticos (son el mismo término de $\mathcal{N}$). $(0^{(m)} = 0^{(n)})$ es, pues, un caso particular del axioma $(E7)$.

▷ Vemos que el conjunto de los términos de $\mathcal{N}$ contiene una sucesión $0, 0^{(1)}, 0^{(2)}, \ldots$ que se interpreta en N como la sucesión de los números naturales. Ahora bien, ciertas *fbf*s. de $\mathcal{N}$ pueden involucrar estos términos, y los teoremas de $\mathcal{N}$ que involucren estos términos se interpretan en N como verdades de la aritmética. El problema general que vamos a investigar hace referencia a la correspondencia entre verdades de la aritmética y teoremas de $\mathcal{N}$. La Proposición 6.1 anterior señala una parte muy limitada de esta correspondencia, pero nos conduce a la idea más general de expresabilidad. Otro ejemplo aclarará más esto.

Ejemplo 6.2

Consideremos la relación $\leqslant$ sobre el conjunto D_N de los números naturales. Intuitivamente, $m \leqslant n$ es la interpretación de la *fbf* $(\exists x_1)(0^{(m)} + x_1 = 0^{(n)})$, con lo que $\leqslant$ queda «expresada» en $\mathcal{N}$ en este sentido. Pero también queda expresada en un sentido más fuerte, puesto que

$$\text{si } m \leqslant n \text{ entonces } \vdash_{\mathcal{N}} (\exists x_1)(0^{(m)} + x_1 = 0^{(n)}),$$

y

$$\text{si } m \not\leqslant n \text{ entonces } \vdash_{\mathcal{N}} \sim (\exists x_1)(0^{(m)} + x_1 = 0^{(n)}).$$

Diciéndolo de otro modo, la relación se cumple o no entre dos números naturales de D_N según si una cierta *fbf* o su negación es un teorema del sistema formal $\mathcal{N}$. En este ejemplo particular omitiremos los detalles de la verificación de que las fórmulas requeridas son teoremas de $\mathcal{N}$.

Definición 6.3

Una relación k-aria R sobre los números naturales es *expresable* en $\mathcal{N}$ si existe una *fbf* $\mathscr{A}(x_1, \ldots, x_k)$ con k variables libres tal que, para todo $n_1, n_2, \ldots, n_k \in D_N$,

(i) Si $R(n_1, \ldots, n_k)$ se verifica en N entonces $\vdash_{\mathcal{N}} \mathscr{A}(0^{(n_1)}, \ldots, 0^{(n_k)})$,

e

(ii) Si $R(n_1, \ldots, n_k)$ no se verifica en N entonces $\vdash_{\mathcal{N}} \sim \mathscr{A}(0^{(n_1)}, \ldots, 0^{(n_k)})$.

Observación 6.4

(*a*) La Proposición 6.1 dice que la relación de igualdad en N es expresable en $\mathcal{N}$ en este sentido preciso.

(*b*) Si supiésemos que $\mathcal{N}$ es completo, la Definición 6.3 podría enunciarse con mayor sencillez, combinando las dos partes (i) e (ii) en un

solo enunciado «si y sólo si», ya que sabríamos que o $\mathscr{A}(0^{(n_1)}, \ldots, 0^{(n_k)})$ o $\sim\mathscr{A}(0^{(n_1)}, \ldots, 0^{(n_k)})$ sería necesariamente un teorema de $\mathscr{N}$. Por lo tanto, las dos condiciones de la Definición 6.3 son necesarias.

(*c*) La argumentación de (*b*) muestra la posibilidad de que no toda *fbf* de $\mathscr{N}$ con variables libres «exprese» una relación de este modo, mientras que toda *fbf* así se interpreta ciertamente como una relación en N.

(*d*) Los conjuntos de números naturales pueden considerarse en este contexto como relaciones monarias. Si A es un subconjunto de D_N, entonces «$\in A$» es una relación monaria sobre D_N que puede o no ser expresable en $\mathscr{N}$ en el sentido arriba definido. Por ejemplo, sea A el conjunto de los números pares. Entonces «$\in A$» es la interpretación de la *fbf*

$$(\exists x_2)(x_2 \times 0^{(2)} = x_1).$$

El lector puede considerar por sí mismo si para cada $m \in D_N$ se tiene que $(\exists x_2)(x_2 \times 0^{(2)} = 0^{(m)})$ o $(\sim(\exists x_2)(x_2 \times 0^{(2)} = 0^{(m)}))$ ha de ser un teorema de $\mathscr{N}$, es decir, si la relación «ser par» es expresable en $\mathscr{N}$.

(*e*) Una función es un tipo particular de relación. En general, una relación $(k+1)$-aria R sobre D_N es una función si, para todo $n_1, \ldots, n_k \in D_N$ existe justamente un $n_{k+1} \in D_N$ tal que se verifica $R(n_1, \ldots, n_k, n_{k+1})$. Al considerar si una función (considerada como relación) es expresable en $\mathscr{N}$ es relevante considerar si la *fbf.* de $\mathscr{N}$ de que se trate comparte esta propiedad de unicidad.

Definición 6.5

Una definición de k argumentos sobre D_N (es decir, una función $D_N^k \to D_N$) es *representable en* $\mathscr{N}$ si es expresable (en cuanto que relación $(k+1)$-aria) en $\mathscr{N}$ mediante una *fbf* $\mathscr{A}$ con $k+1$ variables libres, tal que para todo $n_1, \ldots, n_k \in D_N$.

$$\vdash_{\mathscr{N}} (\exists_1 x_{k+1}) \mathscr{A}(0^{(n_1)}, \ldots, 0^{(n_k)}, x_{k+1})$$

Observación 6.6

Nuevamente hemos de recordar la distinción entre los términos $0^{(n)}$ y los elementos de D_N. A primera vista podría parecer que la condición

$$\vdash_{\mathscr{N}} (\forall x_1) \ldots (\forall x_k)(\exists_1 x_{k+1}) \mathscr{A}(x_1, \ldots, x_k, x_{k+1}) \qquad (*)$$

es equivalente a la condición dada en la Definición. Esto no es así, y el modo más sencillo de ver por qué no tiene por qué ser así es considerar un posible modelo de $\mathscr{N}$ distinto del previsto. Este modelo tendría que contener interpretaciones de todos los términos $0, 0^{(1)}, 0^{(2)}, \ldots$, pero contendría también otros elementos. La interpretación de (*) sería un

enunciado acerca de estos otros elementos, siendo así más fuerte que la conjunción de las interpretaciones de las $(\exists_1 x_{k+1})\mathscr{A}(0^{(n_1)}, \ldots, 0^{(n_k)}x_{k+1})$ para todo $n_1, \ldots, n_k$.

Ejemplo 6.7

La función $f\colon D_N^2 \to D_N$ dada por $f(m, n) = m + n$ es representable en $\mathscr{N}$.

Sea $\mathscr{A}(x_1, x_2, x_3)$ la *fbf.* $x_3 = x_1 + x_2$. Se ha de demostrar lo siguiente, para todo $m, n, p \in D_N$:

(i) si $p = m + n$ entonces $\vdash_{\mathscr{N}} 0^{(p)} = 0^{(m)} + 0^{(n)}$,

(ii) si $p \neq m + n$ entonces $\vdash_{\mathscr{N}} \sim(0^{(p)} = 0^{(m)} + 0^{(n)})$.

e

(iii) $\vdash_{\mathscr{N}} (\exists_1 x_3)(x_3 = 0^{(m)} + 0^{(n)})$.

Podemos demostrar esto del modo siguiente. Sean $m, n \in D_N$. Entonces $\vdash_{\mathscr{N}} 0^{(m)} + 0^{(n)} = 0^{(m+n)}$. En efecto, si $n = 0$, esto es precisamente el axioma ($N3^*$). Si $n > 0$, escribamos $0^{(n)}$ como $(0^{(n-1)})'$. Por ($N4^*$) se tiene entonces:

$$\vdash_{\mathscr{N}} (0^{(m)} + 0^{(n)}) = (0^{(m)} + 0^{(n-1)})'$$

Repitiendo el proceso tantas veces como haga falta, se obtiene:

$$\vdash_{\mathscr{N}} (0^{(m)} + 0^{(n)}) = (0^{(m)} + 0)\overbrace{'' \ldots '}^{n}$$

es decir,

$$\vdash_{\mathscr{N}} (0^{(m)} + 0^{(n)}) = (0\overbrace{'' \cdots '}^{m})\overbrace{'' \cdots '}^{n}$$

es decir,

$$\vdash_{\mathscr{N}} (0^{(m)} + 0^{(n)} = 0^{(m+n)}).$$

(i) e (ii) son ahora consecuencias inmediatas de la Proposición 6.1. Para (iii), hemos de demostrar que:

$$\vdash_{\mathscr{N}} (\exists x_3)(x_3 = 0^{(m)} + 0^{(n)} \wedge (\forall x_i)(x_i = 0^{(m)} + 0^{(n)} \to x_i = x_3))$$

Ahora bien

$$\vdash_{\mathscr{N}} (0^{(m+n)} = 0^{(m)} + 0^{(n)}) \wedge (\forall x_i)(x_i = 0^{(m)} + 0^{(n)} \to x_i = 0^{(m+n)})$$

(Se omiten los detalles, que no son difíciles). Usando el resultado del Ejercicio 3.21, obtenemos el resultado deseado.

Ejemplo 6.8

La función $f\colon D_N \to D_N$ dada por $f(m) = 2m$ es representable en $\mathscr{N}$.

Sea $\mathscr{A}(x_1, x_2)$ la *fbf.* $x_2 = x_1 \times 0^{(2)}$. Hemos de demostrar lo siguiente, para todo $m, n \in D_N$:

(i) si $n = 2m$ entonces $\vdash_{\mathscr{N}} 0^{(n)} = 0^{(m)} \times 0^{(2)}$,

(ii) si $n \neq 2m$ entonces $\vdash_{\mathscr{N}} \sim(0^{(n)} = 0^{(m)} \times 0^{(2)})$,

e

(iii) $\vdash_{\mathscr{N}} (\exists_1 x_2)(x_2 = 0^{(m)} \times 0^{(2)})$.

Para (i), supongamos que $n = 2m$. Vamos a dar el esbozo de una demostración en de $0^{(n)} = 0^{(m)} \times 0^{(2)}$.

$$
\begin{aligned}
0^{(m)} \times 0^{(2)} &= 0^{(m)} \times 0'' && \text{notación}\\
&= (0^{(m)} \times 0') + 0^{(m)} && (N6^*)\\
&= ((0^{(m)} \times 0) + 0^{(m)}) + 0^{(m)} && (N6^*)\\
&= (0 + 0^{(m)}) + 0^{(m)} && (N5^*)\\
&= 0^{(m)} + 0^{(m)} && (N3^*)\\
&= 0^{(m+m)} && \text{por el ejemplo anterior}\\
&= 0^{(2m)}\\
&= 0^{(n)}
\end{aligned}
$$

Para (ii), supongamos que $n \neq 2m$. Entonces $\vdash_{\mathscr{N}} \sim(0^{(2m)} = 0^{(n)})$ por la Proposición 6.1, y $\vdash_{\mathscr{N}} (0^{(2m)} = 0^{(m)} \times 0^{(2)})$ como antes. Usando el axioma $(E9')$ obtenemos entonces $\vdash_{\mathscr{N}} \sim(0^{(m)} \times 0^{(2)} = 0^{(n)})$.

Para (iii), la demostración es como en el ejemplo anterior.

Ejemplo 6.9

La función de dos argumentos Z, definida por $Z(m, n) = 0$ para todo $m, n \in D_N$ es representable en $\mathscr{N}$.

Sea $\mathscr{A}(x_1, x_2, x_3)$ la *fbf*

$$(x_1 = x_1 \wedge x_2 = x_2 \wedge x_3 = 0).$$

De nuevo hemos de verificar que ciertas *fbfs* son teoremas de $\mathscr{N}$:

(i) si $Z(m, n) = p$ entonces $\vdash_{\mathscr{N}} (0^{(m)} = 0^{(m)} \wedge 0^{(n)} = 0^{(n)} \wedge 0^{(p)} = 0)$,

(ii) si $Z(m, n) \neq p$ entonces $\vdash_{\mathscr{N}} \sim(0^{(m)} = 0^{(m)} \wedge 0^{(n)} = 0^{(n)} \wedge 0^{(p)} = 0)$,

e

(iii) $\vdash_{\mathscr{N}} (\exists_1 x_3)(0^{(m)} = 0^{(m)} \wedge 0^{(n)} = 0^{(n)} \wedge x_3 = 0)$,

para todo $m, n, p \in D_N$.

Para (i), si $Z(m, n) = p$ entonces $p = 0$ y $0^{(m)} = 0^{(m)}$, $0^{(n)} = 0^{(n)}$ y $0^{(p)} = 0$ son teoremas de $\mathscr{N}$.

Para (ii), si $Z(m, n) \neq p$, entonces $p \neq 0$, con lo que $\sim(0^{(p)} = 0)$ es un teorema de $\mathscr{N}$ (axioma $(N1^*)$). Se deduce que:

$$\vdash_{\mathscr{N}} \sim(0^{(m)} = 0^{(m)} \wedge 0^{(n)} = 0^{(n)} \wedge 0^{(p)} = 0).$$

Para comprobar (iii) es suficiente demostrar que $\vdash_{\mathscr{N}} (\exists_1 x_3)(x_3 = 0)$, es decir, que $\vdash_{\mathscr{N}} (\exists x_3)(x_3 = 0 \wedge (\forall x_i)(x_i = 0 \rightarrow x_i = x_3))$. Esto se cumple debido a que

$$\vdash_{\mathscr{N}} (0 = 0 \wedge (\forall x_i)(x_i = 0 \rightarrow x_i = 0))$$

Aquí hemos vuelto a usar el resultado del Ejercicio 3.21.

▷ La primera pregunta general que se plantea acerca de funciones representables en $\mathscr{N}$ es si existen funciones que no sean representables de esta manera. Dada una función sobre D_N puede ser difícil comprobar que es representable, y probablemente aún más difícil comprobar que no lo es. Algunas de las dificultades quedan ejemplificadas en lo precedente. Por lo tanto, será útil disponer de resultados generales.

Proposición 6.10

No todas las funciones sobre D_N son representables en $\mathscr{N}$.

Demostración: Compárese con la argumentación de la Observación 5.10(*b*). El conjunto de las *fbfs* de $\mathscr{N}$ es numerable, de modo que el conjunto de las funciones representables en $\mathscr{N}$ es numerable. Pero existe una cantidad no numerable de funciones sobre D_N. Así pues, hay funciones sobre D_N que no son representables en $\mathscr{N}$.

Corolario 6.11

No todas las relaciones sobre D_N son expresables en $\mathscr{N}$.

Demostración: Análoga a la anterior.

▷ La siguiente cuestión que parece lógico plantear es: ¿podemos caracterizar el conjunto de funciones (relaciones) sobre D_N que son representables (expresables) en $\mathscr{N}$? La respuesta es un resultado importante, y una de las claves del teorema de Gödel referente a la incompletitud del sistema $\mathscr{N}$.

Proposición 6.12

Una función (relación) sobre D_N es representable (expresable) en $\mathscr{N}$ si y sólo si es recursiva.

Por supuesto, esto todavía no significa nada para nosotros, e incluso la demostración completa cae fuera de nuestro alcance; pero una vez que hayamos definido y descrito las funciones y relaciones recursivas, veremos la importancia del resultado.

Ejercicios

1 Demuéstrese que para todo m, $n \in D_N$, si $m \leqslant n$, entonces
$\vdash_{\mathscr{N}} (\exists x_1)(0^{(m)} + x_1 = 0^{(n)})$.

2 Demuéstrese que, para todo m, $n \in D_N$, si $m > n$, entonces

$$\vdash_{\overline{\mathcal{N}}} \sim(\exists x_1)(0^{(m)} + x_1 = 0^{(n)}).$$

3 Escríbanse *fbfs* del sistema $\mathcal{N}$ cuyas interpretaciones en N sean las siguientes:
(*a*) n no es un número primo;
(*b*) m y n no tienen factores primos comunes;
(*c*) $m = \min(p, q)$;
(*d*) todo $m \in D_N$ tiene un factor primo;
(*e*) $sg(m) = n$ (para la definición, véase pág. 136).

4 Demuéstrese que las siguientes funciones sobre D_N son representables en $\mathcal{N}$, sin usar la Proposición 6.12.
(*a*) sg (para la definición, véase pág. 136);
(*b*) f, siendo $f(n) = n + 3$;
(*c*) rs_2, siendo $rs_2(n)$ el resto de la división de n entre 2.

5 Demuéstrese que una función $f: D_N \to D_N$ es representable en $\mathcal{N}$ si existe una *fbf* $\mathscr{A}$ de $\mathcal{N}$ tal que
(i) Si $f(m) = n$ entonces $\vdash_{\overline{\mathcal{N}}} \mathscr{A}(0^{(m)}, 0^{(n)})$,
e
(ii) Para todo $m \in D_N$, $\vdash_{\overline{\mathcal{N}}} (\exists_1 x_2)\mathscr{A}(0^{(m)}, x_2)$
(Esto se extiende a funciones de cualquier número de variables).

6 Demuéstrese que la función de proyección $p_i^k: D_N^k \to D_N$, dada por $p_i^k(n_1, \ldots, n_k) = n_i (n_1, \ldots, n_k \in D_N)$ es representable en $\mathcal{N}$, para todo i, $k > 0$.

6.3 Funciones y relaciones recursivas

La clase de las funciones recursivas se define (sin hacer referencia al sistema $\mathcal{N}$) del siguiente modo: Ciertas funciones que pueden definirse fácilmente son recursivas, y todas las funciones obtenidas a partir de estas mediante la aplicación de tres reglas son también recursivas.

Las funciones básicas son:

1. La función cero $z: D_N \to D_N$, dada por $z(n) = 0$ para todo $n \in D_N$.

2. La función sucesor $s: D_N \to D_N$, dada por $s(n) = n + 1$, para todo $n \in D_N$.

3. Las funciones de proyección $p_i^k: D_N^k \to D_N$, dadas por $p_i^k(n_1, \ldots, n_k) = n_i$, para todo $n_1, \ldots, n_k \in D_N$. Nótese que p_1^1 es la función identidad.

Las tres reglas son:

I. Composición. Si $g: D_N^j \to D_N$ y $h_i: D_N^k \to D_N$ para $1 \leqslant i \leqslant j$, entonces $f: D_N^k \to D_N$ definida por:

$$f(n_1, \ldots, n_k) = g(h_1(n_1, \ldots, n_k), \ldots, h_j(n_1, \ldots, n_k))$$

se obtiene mediante composición a partir de g y $h_1, \ldots, h_j$.

II. Recursión. Si $g: D_N^k \to D_N$ y $h: D_N^{k+2} \to D_N$, entonces la función $f: D_N^{k+1} \to D_N$ definida por

$$f(n_1, \ldots, n_k, 0) = g(n_1, \ldots, n_k)$$

$$f(n_1, \ldots, n_k, n+1) = h(n_1, \ldots, n_k, n, f(n_1, \ldots, n_k, n))$$

se dice que está obtenida mediante recursión a partir de g y h. Nótese que aquí $n_1, \ldots, n_k$ son parámetros que no afectan a la definición, por lo cual permitiremos omitirlos. La función f definida por

$$f(0) = a \text{ (elemento fijo de } D_N)$$

y

$$f(n+1) = h(n, f(n))$$

también está obtenida mediante recursión.

III. Operador de minimización. Sea $g: D_N^{k+1} \to D_N$ cualquier función que tenga la propiedad de que para todo $n_1, \ldots, n_k \in D_N$ existe al menos un $n \in D_N$ tal que $g(n_1, \ldots, n_k, n) = 0$. Entonces la función $f: D_N^k \to D_N$, definida por

$$f(n_1, \ldots, n_k) = \text{mínimo número } n \in D_N \text{ tal que } g(n_1, \ldots, n_k, n) = 0$$

se dice que está obtenida a partir de g mediante uso del operador de minimización.

Notación: El menor número n tal que $g(n_1, \ldots, n_k, n) = 0$ se denota por

$$\mu n [g(n_1, \ldots, n_k, n) = 0].$$

Observación 6.13

La condición impuesta a g de que para todo $n_1, \ldots, n_k$ exista al menos un n tal que $g(n_1, \ldots, n_k, n) = 0$ es claramente necesaria para asegurar que la función f sea total, es decir, tenga un valor para cada k-tupla de números naturales. Más tarde tendremos ocasión de permitir el uso del operador de minimización sin esta condición. Ello llevará obviamente a la introducción de funciones parciales. Por el momento, no obstante, mantendremos la condición y todas nuestras funciones serán funciones totales.

Ejemplo 6.14

(*a*) La función $f: D_N^3 \to D_N$ dada por $f(m, n) = m^2 + mn$ se ha obtenido mediante composición a partir de las funciones de adición, multiplicación y proyección, ya que (suponiendo que f_1 denote la suma y f_2 denote el producto):

$$f(m, n) = f_2(p_1^2(m, n), f_1(m, n))$$

(*b*) La función $g: D_N^3 \to D_N$ dada por $g(m, n, p) = n^2$ se ha obtenido mediante composición, ya que

$$g(m, n, p) = f_2(p_2^3(m, n, p), p_2^3(m, n, p))$$

suponiendo que f_2 denote al producto.

(*c*) La función de adición se obtiene mediante recursión a partir de p_1^1 y la composición de s con p_3^3, ya que

$$f_1(m, 0) = p_1^1(m)$$
$$f_1(m, n+1) = s(p_3^3(m, n, f_1(m, n)))$$

(*d*) Análogamente, la función de multiplicación se obtiene por recursión a partir de la función de adición.

(*e*) Sea $f(n) =$ mínimo número q tal que $n+q \equiv 0 \pmod{p}$ ($n, p, q \in D_N$). Entonces f se obtiene mediante el operador de minimización a partir de la función g, siendo $g(n, p, q) =$ el resto de la división de $n+q$ entre p.

Definición 6.15

Una función sobre D_N es *recursiva* si puede obtenerse a partir de las funciones de 1, 2, 3 de más arriba mediante un número finito de aplicaciones de las reglas I, II, III. La clase de las funciones recursivas es pues la menor clase de funciones sobre D_N que contiene a todas las funciones de 1, 2, 3 y es cerrada bajo la aplicación de las reglas I, II, III.

Una función *recursiva primitiva* si puede obtenerse a partir de las funciones de 1, 2, 3 mediante un número finito de aplicaciones de las reglas I y II solamente. Las funciones recursivas primitivas forman una clase estrictamente menor que las funciones recursivas (esto requiere una demostración en la que no entraremos). Son importantes en algunas ramas de esta materia, pero nosotros no tendremos necesidad de considerarlas específicamente.

Ejemplo 6.16

(*a*) La función suma es recursiva (primitiva). Para verlo, volvamos al Ejemplo 6.14(*c*), donde la función suma se obtiene por recursión a partir de una función de proyección y de la función sucesor.

(*b*) La función producto es recursiva (primitiva). Para verlo, definamos $f_2: D_N^2 \to D_N$ del modo siguiente:

$$f_2(m, 0) = z(m)$$
$$f_2(m, n+1) = h(m, n, f_2(m, n))$$

siendo $h(m, n, p) = f_1(p_3^3(m, n, p), p_1^3(m, n, p))$. f_2 queda así definida por

recursión a partir de z, que es recursiva, y de h, que es recursiva, por estar obtenida mediante composición a partir de f_1, p_3^3 y p_1^3.

(*c*) El ejemplo 6.14(*b*) muestra una función recursiva.

(*d*) La función $f: D_N \to D_N$ dada por $f(n) = n!$ es recursiva (primitiva). En efecto, f está definida por

$$f(0) = 1$$
$$f(n+1) = f_2(s(n), f(n)),$$

estando así obtenida mediante recursión (y composición) a partir de la función sucesor y la función de multiplicación, que son recursivas (primitivas).

(*e*) Todas las funciones constantes son recursivas. La función constante de valor k puede definirse a partir de la función de proyección p_2^2 como

$$f(0) = k$$
$$f(n+1) = p_2^2(n, f(n))$$

Usando otras funciones de proyección puede verse que las funciones constantes de más de un argumento son también recursivas.

(*f*) Las funciones sg, $\overline{sg}: D_N \to D_N$ dadas por

$$sg(n) = \begin{cases} 0 \text{ si } n = 0 \\ 1 \text{ si } n \neq 0 \end{cases} \qquad \overline{sg}(n) = \begin{cases} 1 \text{ si } n = 0 \\ 0 \text{ si } n \neq 0 \end{cases}$$

son recursivas, ya que

$$sg(0) = 0$$
$$sg(n+1) = 1 \text{ (la función constante)}$$

y

$$\overline{sg}(0) = 1$$
$$\overline{sg}(n+1) = 0$$

▷ Podría parecer que esta definición es tan engorrosa de aplicar como la definición de función representable en $\mathcal{N}$, pero ello no es así, y la naturaleza inductiva de la definición permite construir rápida y fácilmente amplias colecciones de funciones recursivas. No obstante, existe otro beneficio que aparece en conexión con la recursividad y que concierne a la *computabilidad* de la que hablaremos más tarde.

La noción de recursividad se extiende a relaciones mediante la idea de función característica.

Definición 6.17

Sea R una relación de k argumentos sobre D_N. La *función característica* de R (denotada por C_R) se define como

$$C_R(n_1, \ldots, n_k) = \begin{cases} 0 & \text{si se verifica } R(n_1, \ldots, n_k) \\ 1 & \text{si no se verifica } R(n_1, \ldots, n_k) \end{cases}$$

Definición 6.18

Una relación R sobre D_N es *recursiva* si su función característica es recursiva.

Ejemplo 6.19

La relación binaria R, tal que $R(m, n)$ se verifica si y sólo si $m+n$ es par, es recursiva.

Para demostrarlo, hemos de mostrar que la función f definida por

$$f(m, n) = \begin{cases} 0 & \text{si } m+n \text{ es par} \\ 1 & \text{si } m+n \text{ es impar} \end{cases}$$

es recursiva. Sea rs_2: $D_N \to D_N$ la función dada por $rs_2(n)$ = resto de la división de n entre 2. rs_2 es recursiva, ya que

$$rs_2(0) = 0$$
$$rs_2(n+1) = \overline{sg}\,(rs_2(n)) = \overline{sg}\,(p_2^2(n, rs_2(n))).$$

Ahora bien, $f(m, n) = rs_2(m+n)$, luego f es recursiva por composición, ya que $+$ y rs_2 son recursivas.

Ejemplo 6.20

La relación $\leqslant$ es recursiva.

Para demostrarlo hemos de mostrar que la función g definida por

$$g(m, n) = \begin{cases} 0 & \text{si } m \leqslant n \\ 1 & \text{si } m > n \end{cases}$$

es recursiva. Esto requiere varios pasos. Primero, la función p, definida por

$$p(n) = \begin{cases} n-1 & \text{si } n > 0 \\ 0 & \text{si } n = 0 \end{cases}$$

es recursiva. Para verlo,

$$\left.\begin{aligned} p(0) &= 0 \\ p(n+1) &= n \end{aligned}\right\} \text{ usando recursión.}$$

Seguidamente, la función $\dot{-}$, definida por

$$m \dot{-} n = \begin{cases} m-n & \text{si } m \geqslant n \\ 0 & \text{si } n > m \end{cases}$$

es recursiva. Para verlo,

$$\left.\begin{aligned} m \dot{-} n &= m \\ m \dot{-} (n+1) &= p(m \dot{-} n) \end{aligned}\right\} \text{ usando recursión.}$$

Nótese que la función sustracción no puede discutirse aquí, porque conduce a valores negativos, y nuestro dominio numérico consta de los enteros no negativos. La función denotada por $\dot{-}$ es una sustracción modificada.

Ahora podemos ver cómo definir g del modo requerido.

$$g(m,\ n) = sg(m \dot{-} n), \text{ usando composición.}$$

▷ La definición de recursividad puede aplicarse también a conjuntos de números. Dado $A \subseteq D_N$, diremos que A es recursivo si la función característica de A es recursiva. (La función característica de un conjunto A es, precisamente, la función característica, en el sentido definido más arriba, de la relación « $\in A$».)

Ejemplo 6.21

(*a*) El conjunto D_N es recursivo, puesto que su función característica es la función cero, que es recursiva.

(*b*) $\varnothing$ es recursivo, ya que su función característica es una función constante.

(*c*) El conjunto de los números pares es recursivo. Para verlo hemos de demostrar que la función h dada por

$$h(n) = \begin{cases} 0 & \text{si } n \text{ es par} \\ 1 & \text{si } n \text{ es impar} \end{cases}$$

es recursiva. Pero h es precisamente la función rs_2 definida en el ejemplo 6.19.

Proposición 6.22

Si R y S son relaciones recursivas de k argumentos, entonces las relaciones $\bar{R}$, $R \wedge S$ y $R \vee S$ son recursivas. ($\bar{R}$ es la relación que se verifica para una k-tupla dada si y sólo si R no se verifica para esa k-tupla. $R \wedge S$ se cumple para una k-tupla dada si y sólo si tanto R como S se verifican. $R \vee S$ se cumple para una k-tupla dada si y sólo si R ó S se verifican.)

Demostración: La función característica de $\bar{R}$ es $\overline{sg}(C_R)$, de modo que es recursiva supuesto que C_R sea recursiva. Asimismo

$$C_{R \wedge S}(n_1, \ldots, n_k) = sg(C_R(n_1, \ldots, n_k) + C_S(n_1, \ldots, n_k))$$

y

$$C_{R \vee S}(n_1, \ldots, n_k) = C_R(n_1, \ldots, n_k) \times C_S(n_1, \ldots, n_k).$$

Por lo tanto, $C_{R \wedge S}$ y $C_{R \vee S}$ son recursivas, supuesto que C_R y C_S sean recursivas.

Corolario 6.23

Para conjuntos recursivos cualesquiera A y B, el complemento de A, la intersección de A y B, y la unión de A y B son conjuntos recursivos.

Demostración: Este resultado no es más que un caso especial de la proposición, ya que los conjuntos A y B tienen funciones características que son las funciones características de las relaciones « $\in A$» y « $\in B$».

▷A partir de aquí puede procederse a demostrar la recursividad de funciones, relaciones y conjuntos particulares, y de hecho es necesario hacerlo así para demostrar la Proposición 6.12 y la incompletitud del sistema $\mathcal{N}$. De hecho, es más difícil encontrar una función o relación que *no sea* recursiva, ya que virtualmente todas las funciones y relaciones fácilmente describibles son recursivas. Llevaremos a cabo este proceso hasta cierto punto, a fin de comunicar una impresión de los procedimientos involucrados y al hacerlo surgirá alguna idea de las dificultades de describir una función o relación no recursiva.

Proposición 6.24

Todo conjunto unitario de D_N es recursivo.

Demostración: Hemos de demostrar que, para todo $k \in D_N$, la función $S_k : D_N \to D_N$ dada por

$$S_k(n) = \begin{cases} 0 & \text{si } n = k \\ 1 & \text{en otro caso} \end{cases}$$

es recursiva. La hacemos por inducción sobre k.

Paso base:

$$S_0(n) = \begin{cases} 0 & \text{si } n = 0 \\ 1 & \text{si } n \neq 0 \end{cases}$$

S_0 es precisamente la función *sg*, de modo que es recursiva.

Paso de inducción: Sea $k > 0$ y supongamos que S_{k-1} es recursiva

$$S_k(n) = \begin{cases} 0 & \text{si } n = k \\ 1 & \text{si } n \neq k \end{cases}$$

luego tenemos

$$S_k(0) = 1$$

y

$$S_k(n+1) = S_{k-1}(n) \text{ para todo } n \in D_N.$$

Así pues, S_k está obtenida por recursión a partir de S_{k-1}, con lo cual es recursiva.

Por tanto, por inducción, S_k es recursiva para todo $k \in D_N$, lo que prueba el resultado.

Ejemplo 6.25

(*a*) Todo conjunto finito es recursivo. Esto es consecuencia de la Proposición 6.24 y el Corolario 6.23, ya que un conjunto finito puede escribirse como unión finita de conjuntos unitarios.

(*b*) Definamos $p : D_N \to D_N$ poniendo

$$p(n) = n\text{-ésimo número primo impar, si } n > 0,$$

y

$$p(0) = 2.$$

Entonces p es una función recursiva. Esto puede parecer sorprendente, ya que se sabe que p no posee expresión algebraica sencilla. No obstante, puede demostrarse a partir de la definición (con un cierto número de pasos intermedios) que p cae dentro de la clase de las funciones recursivas.

(*c*) De acuerdo con la teoría de números elemental, todo número natural puede expresarse unívocamente como producto de potencias de números primos. Definamos, para cada $i \in D_N$, una función e_i poniendo:

$$e_i(n) = \begin{cases} \text{exponente del número primo } p(i) \text{ en la expresión} \\ \text{de } n \text{ como producto de potencias de primos, si} \\ p(i) \text{ aparece en dicha expresión. 0 en otro caso.} \end{cases}$$

Entonces e_i es una función recursiva para todo i.

(*d*) La función $d: D_N^2 \to D_N$ tal que

$$d(m, n) = \text{el máximo común divisor de } m \text{ y } n,$$

es recursiva.

▷A partir de funciones básicas y reglas sencillas pueden construirse funciones recursivas complicadas, y es evidente que no hay ningún límite de complejidad en la aplicación de las reglas I, II y III. La demostración de la Proposición 6.12, que puede encontrarse en Mendelson, es bastante tediosa y depende considerablemente de demostraciones de que ciertas funciones y relaciones particulares son recursivas, y de resultados acerca de cómo pueden combinarse funciones recursivas para dar otras funciones y relaciones recursivas.

Como corolario de las Proposiciones 6.10 y 6.12, podemos obtener el resultado, más bien inútil, de que no todas las funciones sobre D_N son recursivas. De hecho, esto puede demostrarse más directamente mediante un argumento de numerabilidad, sin usar estas proposiciones.

El conjunto de las funciones recursivas es numerable, y este hecho nos permite construir una función que no es recursiva. Consideremos una enumeración $f_1, f_2, \ldots$ de todas las funciones recursivas de un argumento. Definamos una función $g: D_N^2 \to D_N$ poniendo

$$g(m, n) = f_m(n)$$

Entonces g es una función no recursiva. En efecto, supongamos que g fuese recursiva. Definamos h poniendo

$$h(m) = g(m, m) + 1 \qquad (m \in D_N)$$

h es recursiva por serlo g, y por lo tanto h es idéntica a f_k, para algún k. Para este k tenemos

$$h(k) = f_k(k) = g(k, k) + 1 = f_k(k) + 1$$

De esta contradicción deducimos que g no es recursiva.

Ejercicios

7 Demuéstrese que las siguientes funciones son recursivas.

(*a*) $e: D_N^2 \to D_N$, dada por $e(m, n) = m^n$.

(*b*) $\min: D_N \to D_N$, dada por

$$\min(m, n) = \begin{cases} m & \text{si } m \leqslant n \\ n & \text{si } m > n. \end{cases}$$

(*c*) $q: D_N^2 \to D_N$, dada por

$$q(m, n) = \begin{cases} \text{cociente de la división de } n \text{ entre } m & \text{si } m \neq 0 \\ 0 & \text{si } m = 0. \end{cases}$$

8 Sea R una relación recursiva de $k+1$ argumentos tal que para todo n_1, ..., $n_k \in D_N$ existe al menos un $n_{k+1} \in D_N$ tal que se verifica $R(n_1, ..., n_k, n_{k+1})$. Demuéstrese que la función f definida por $f(n_1, ..., n_k) = \mu x[R(n_1, ..., n_k, x)]$ $(n_1, ..., n_k \in D_N)$ es recursiva.

9 Sea $e_2 : D_N \to D_N$ dada por:

$e_2(n)$ = exponente de 2 en la expresión de n como producto de potencias de números primos.

($e_2(n) = 0$ si 2 no aparece en esa expresión.)

Demuéstrese que e_2 es una función recursiva.

10 Repítase el Ejercicio 9, reemplazando e_2 por la función e_k cuyo valor es el exponente del número primo p_k (k fijo).

11 Sean f y g funciones recursivas. Demuéstrese que la función h dada por

$$h(x) = f(x)^{g(x)} \qquad (x \in D_N)$$

es recursiva.

12 Demuéstrese que, para todo $n > 1$, si $R_1, \ldots, R_n$ son relaciones recursivas de k argumentos, entonces $R_1 \wedge \ldots \wedge R_n$ y $R_1 \vee \ldots \vee R_n$ son relaciones recursivas.

13 Demuéstrese que, para $n > 1$, si $A_1, \ldots, A_n$ son conjuntos recursivos, entonces $A_1 \cap \ldots \cap A_n$ y $A_1 \cup \ldots \cup A_n$ son conjuntos recursivos.

14 Sea R una relación binaria sobre D_N y sea k un número natural fijo. Definanse relaciones monarias (es decir, predicados) sobre D_N como sigue:

$S(n)$ se verifica si y sólo si existe $m < k$ tal que se verifica $R(m, n)$.
$T(n)$ se verifica si y sólo si $R(m, n)$ se verifica para todo $m < k$.

Demuéstrese que si R es una relación recursiva, S y T lo son también. ¿Puede modificarse la demostración para aplicarla al caso en que se elimina la condición «$< k$»?

6.4 Números de Gödel

Una de las técnicas esenciales que utilizó Gödel en la demostración de la incomplitud de $\mathcal{N}$ se ha convertido en un procedimiento standard en lógica y en otros campos. La idea es la de *números de código*. Generalmente, la información puede presentarse en el lenguaje castellano, o en otro lenguaje natural, o en un lenguaje simbólico abstracto. Para discutir, transmitir o procesar esta información puede ser conveniente (e incluso esencial) el ponerla en forma numérica. Por ejemplo, cuando la información ha de ser procesada por una máquina, es frecuente convertirla primero en algún tipo de información numérica. Para ejemplificar de un modo burdo cómo se podría hacer esto, supongamos que las palabras de un cierto diccionario se numeran en orden, de 20 en adelante (por ejemplo). A los signos de puntuación habituales podrían asignárseles números menores que 20. Una frase duda podría escribirse entonces como una sucesión finita de números.

Lo que Gödel hizo fue una construcción similar para el lenguaje de primer orden $\mathscr{L}$ (todavía arbitrario y no especificado), de tal manera que a cada símbolo, término, *fbf* y sucesión finita de *fbfs* de $\mathscr{L}$ se le asigna un número de código, de modo que partiendo de cualquier número de código dado, la correspondiente expresión de $\mathscr{L}$ es fácilmente recuperable. Hay diferentes maneras de hacer esto; nosotros vamos a describir una de ellas.

Primeramente, definamos una función g sobre el conjunto de símbolos de $\mathscr{L}$ así:

$$g((\,)=3,$$
$$g())=5,$$
$$g(,)=7,$$
$$g(\sim)=9$$
$$g(\rightarrow)=11,$$
$$g(\forall)=13,$$
$$g(x_k)=7+8k \text{ para } k=1, 2, \ldots,$$
$$g(a_k)=9+8k \text{ para } k=1, 2, \ldots,$$
$$g(f_k^n)=11+8x(2^n\times 3^k) \text{ para } n=1, 2, \ldots; k=1, 2, \ldots,$$
$$g(A_k^n)=13+8x(2^n\times 3^k) \text{ para } n=1, 2, \ldots$$

Nótese que a cada símbolo se le asigna un número entero positivo impar diferente. Nótese también que todo número entero positivo impar (que corresponda a algún símbolo) puede descomponerse fácilmente para encontrar el símbolo del que procede.

Ejemplo 6.26

(*a*) Encuéntrese el símbolo (si existe) correspondiente al número 587.

Si 587 corresponde a algún símbolo, debería ser uno de entre x_k, a_k, f_k^n o A_k^n, de modo que primero hemos de encontrar el resto de la división entre 8.

$$587=8\times 73+3=8\times 72+11$$

y $72=2^3\times 3^2$, así que 587 corresponde a la letra de función f_2^3.

(*b*) Demuéstrese que 333 no corresponde a ningún símbolo de $\mathscr{L}$.

$$333=8\times 41+5=8\times 40+13,$$

pero $40 = 2^3 \times 5$, que no es de la forma $2^n \times 3^k$, así que 333 no corresponde a ningún símbolo de $\mathscr{L}$.

▷ Por supuesto, en un lenguaje $\mathscr{L}$ particular no aparecerán todos los símbolos de manera que no se utilizarán todos los números de código.

Ahora tenemos que un término o una *fbf* de $\mathscr{L}$ es una cadena de símbolos de $\mathscr{L}$, y podemos asignar números a tales cadenas del siguiente modo. Si $u_1, \ldots, u_k$ son símbolos de $\mathscr{L}$, denotemos por $u_1, u_2, \ldots, u_k$ la cadena de símbolos (que puede ser o no un término o *fbf* de $\mathscr{L}$) y definamos

$$g(u_1, u^2, \ldots, uk) = 2^{g(u_1)} \times 3^{g(u_2)} \times \ldots \times p_k^{g(u_k)}$$

donde, para cada $i > 0$, p_i denota al i-ésimo número primo impar, y $p_0 = 2$. Puesto que cada número puede expresarse unívocamente como producto de potencias de primos, existe un procedimiento obvio para hallar la cadena de símbolos (si la hay) correspondiente a un número dado. Además, diferentes cadenas de símbolos tendrán necesariamente diferentes números de código.

Ejemplo 6.27

(*a*) $$g(f_1^1(x_1)) = 2^{g(f_1^1)} \times 3^{g(()} \times 5^{g(x_1)} \times 7^{g())}$$
$$= 2^{59} \times 3^3 \times 5^{15} \times 7^5.$$

(*b*) $$g((A_1^2(x_1, x_2) \rightarrow A_1^1(x_1)))$$
$$= 2^{g(()} \times 3^{g(A_1^2)} \times 5^{g(()} \times 7^{g(x_1)} \times 11^{g(,)} \times 13^{g(x_2)} \times 17^{g())}$$
$$\times 19^{g(\rightarrow)} \times 23^{g(A_1^1)} \times 29^{g(()} \times 31^{g(x_1)} \times 37^{g())} \times 41^{g(())}$$
$$= 2^3 \times 3^{109} \times 5^3 \times 17^{15} \times 11^7 \times 13^{23} \times 17^5 \times 19^{11} \times 23^{61} \times 29^3$$
$$\times 31^{15} \times 37^5 \times 41^5.$$

(*c*) Todo número en el que aparezca un número primo elevado a una potencia par, o tal que haya huecos en la sucesión de primos que intervienen, no puede corresponder a ninguna cadena de símbolos.

Observación 6.28

Los números de código de símbolos son números impares. Los números de código de cadenas de símbolos son números pares (ya que el número primo 2 aparece siempre con exponente no nulo en el número de código de toda cadena). Así pues, las dos clases de números de código pueden distinguirse fácilmente.

▷ Es posible asignar números de código a sucesiones finitas de cadenas de símbolos mediante una posterior extensión de este proceso. Sean s_1, s_2, ..., s_r cadenas de símbolos de $\mathscr{L}$, y definamos

$$g(s_1, s_2, \ldots, s_r) = 2^{g(s_1)} \times 3^{g(s_2)} \times \ldots \times p_r^{g(s_r)}$$

Nótese que un número dado no puede ser el número de código de una sucesión finita en este sentido, y a la vez el número de código de una cadena de símbolos, puesto que el exponente de 2 es par en los números de código de sucesiones finitas e impar en los números de código de cadenas (por la Observación 6.28).

Hemos definido así una función g, cuyo dominio es el conjunto de todos los símbolos, cadenas de símbolos y sucesiones finitas de cadenas de símbolos de $\mathscr{L}$, y que toma valores en D_N. Esta función es inyectiva, pero no sobreyectiva, como hemos visto. Ha sido definida de tal manera que existe un procedimiento efectivo (consistente en hacer uso de la expresión de un número como producto de potencias de números primos) para calcular g^{-1} para cualquier número del rango de g. Llamaremos a los valores de g números de Gödel. Todo término o *fbf* de $\mathscr{L}$ es una cadena de símbolos, por lo que tiene un número de Gödel. Una demostración o deducción de $K_{\mathscr{L}}$ es una sucesión finita de cadenas de símbolos, y tiene por lo tanto un número de Gödel.

El propósito que Gödel perseguía al diseñar este sistema de codificación era transformar aserciones acerca de un sistema formal (por ejemplo, $\mathscr{N}$) en aserciones acerca de números, a fin de expresar dichas aserciones dentro del sistema formal. Las aserciones que pueden hacerse acerca de un sistema formal conciernen a *fbfs*, teoremas y demostraciones. Por ejemplo: 'La sucesión $\mathscr{A}_1, \ldots, \mathscr{A}_k, \mathscr{A}$ es una demostración en $\mathscr{N}$ de la *fbf* $\mathscr{A}$'. Esta aserción afirma que se verifica una cierta relación entre una sucesión finita de *fbfs* y una cierta *fbf*. A través de los números de Gödel esto da lugar a una relación sobre D_N, llamémosla $\mathscr{D}m$, definida por: $\mathscr{D}m(m, n)$ se verifica si y sólo si m es el número de Gödel de una sucesión finita de *fbfs* de $\mathscr{N}$ que constituye una demostración en $\mathscr{N}$ de la *fbf* de número de Gödel n.

Otras propiedades de $\mathscr{N}$ y aserciones acerca de $\mathscr{N}$ dan lugar de manera similar a relaciones sobre D_N. Aquí es donde cobra importancia la cuestión de la expresabilidad, ya que, volviendo al ejemplo anterior, si la relación $\mathscr{D}m$ fuese expresable en $\mathscr{N}$ existiría una *fbf* $\mathscr{P}(x_1, x_2)$ de $\mathscr{L}_N$ tal que para todo $m, n \in D_N$:

si $\mathscr{D}m(m, n)$ se verifica entonces $\vdash_{\mathscr{N}} \mathscr{P}(0^{(m)}, 0^{(n)})$,

y

$\mathscr{D}m(m, n)$ no se verifica entonces $\vdash_{\mathscr{N}} \sim \mathscr{P}(0^{(m)}, 0^{(n)})$

Diciéndolo más groseramente, habría una *fbf* $\mathscr{P}(x_1, x_2)$ que decidiría *dentro del sistema* el 'metaproblema' de si una sucesión finita arbitraria $\mathscr{A}_1, \ldots, \mathscr{A}_k, \mathscr{A}$ de *fbfs* constituye una demostración en $\mathscr{N}$. Lo que estamos haciendo equivale a un intento de usar el sistema $\mathscr{N}$ (al menos parcialmente) como metasistema, en el sentido discutido en capítulos anteriores, para sí mismo. En vista de ello, el procedimiento parece peligroso y propenso a llevar a contradicciones; pero sabemos que tan sólo las relaciones recursivas sobre D_N son expresables en $\mathscr{N}$, de manera que el procedimiento no puede llevarse a cabo para todas las relaciones sobre D_N, y el uso de $\mathscr{N}$ como metasistema para sí mismo será necesariamente parcial. A causa de esto, es posible evitar contradicciones.

El siguiente paso de la demostración del teorema de Gödel es demostrar que ciertas relaciones sobre D_N que surgen de este modo a partir de consideraciones acerca de *fbfs*, teoremas y demostraciones, son recursivas, y con ello expresables en $\mathscr{N}$. Omitiremos los detalles, limitándonos a enumerar algunas de estas relaciones.

Proposición 6.29

Las siguientes relaciones sobre D_N son recursivas, y con ello expresables en $\mathscr{N}$.

(i) *Fbf* *Fbf*(n) se verifica si y sólo si n es el número de Gödel de una *fbf.* de $\mathscr{N}$.

(ii) *Lax* *Lax*(n) se verifica si y sólo si n es el número de Gödel de un axioma lógico de $\mathscr{N}$.

(iii) *Prax* *Prax*(n) se verifica si y sólo si n es el número de Gödel de un axioma propio de $\mathscr{N}$.

(iv) *Dmt* *Dmt*(n) se verifica si y sólo si n es el número de Gödel de una demostración en $\mathscr{N}$.

(v) *Dm* *Dm*(m,n) se verifica si y sólo si m es el número de Gödel de una demostración de la *fbf.* de número de Gödel n.

(vi) *Subst* *Subst*(m, n, p, q) se verifica si y sólo si m es el número de Gödel del resultado de sustituir el término de número de Gödel p en el lugar de todas las intervenciones libres de la variable de número de Gödel q en la expresión de número de Gödel n.

(vii) *W* $W(m, n)$ se verifica si y sólo si m es el número de Gödel de una *fbf* $\mathscr{A}(x_1)$ en la que aparece libre x_1, y n es el número de Gödel de una demostración de $\mathscr{A}(0^{(m)})$ en $\mathscr{N}$.

(viii) *D* $D(m,n)$ se verifica si y sólo si m es el número de Gödel de una *fbf.* $\mathscr{A}(x_1)$ en la que aparezca libre la variable x_1, y n es el número de Gödel de la *fbf* $\mathscr{A}(0^{(m)})$

Ejercicios

15 Encuéntrense los símbolos de $\mathscr{L}$ correspondientes a los números de código siguientes:
(*a*) 65 (*b*) 299
(*c*) 109 (*d*) 421.

16 Encuéntrense las *fbfs* de $\mathscr{L}$ correspondientes a los números de código siguientes:
(*a*) $2^{61} \times 3^3 \times 5^{15} \times 7^5$;
(*b*) $2^9 \times 3^{61} \times 5^3 \times 7^{15} \times 11^5$;
(*c*) $2^3 \times 3^{13} \times 5^{15} \times 7^5 \times 11^{61} \times 13^3 \times 17^{15} \times 19^5$.

17 Todo número corresponde a una única sucesión finita de números naturales, determinada por su expresión como producto de potencias de números primos. Por ejemplo, el número $2^4 \times 3 \times 5^7 \times 11^2$ corresponde a la sucesión finita 4, 1, 7, 0, 2. Dos sucesiones finitas pueden combinarse mediante concatenación, es decir, extendiéndose una de ellas mediante yuxtaposición de los miembros de la otra. Por ejemplo, si s es la sucesión 2, 3, 5 y t es la sucesión 4, 7, 9, 10, denotamos por $s * t$ a la sucesión 2, 3, 5, 4, 7, 9, 10. Defínase una función f: $D_N^2 \rightarrow D_N$ poniendo:

$f(m,n)$ = el número de código de $s * t$, siendo s y t las sucesiones cuyos números de código son m y n.

Demuéstrese que f es recursiva.

6.5 La demostración de incompletitud

La relación W definida en la Proposición 6.29 es la clase de demostración de incompletitud, así que hemos de esforzarnos en comprender su significado. Nótese que W involucra la sustitución del término $0^{(m)}$ (correspondiente al número m) en la *fbf* $\mathscr{A}(x_1)$, cuyo número de Gödel es m.

W es expresable en $\mathscr{N}$, de modo que existe una *fbf* $\mathscr{W}(x_1, x_2)$ en la que solamente figuraban libres x_1 y x_2, tal que

si se verifica $W(m,n)$, entonces $\vdash_{\mathscr{N}} \mathscr{W}(0^{(m)}, 0^{(n)})$

y

si no se verifica $W(m,n)$, entonces $\vdash_{\mathscr{N}} \sim \mathscr{W}(0^{(m)}, 0^{(n)})$

Consideremos la *fbf*

$$(\forall x_2) \sim \mathscr{W}(x_1, x_2)$$

Sea p el número de Gödel de esta *fbf* y consideremos finalmente la *fbf* obtenida sustituyendo $0^{(p)}$ en el lugar de x_1, es decir

$$(\forall x_2) \sim \mathscr{W}(0^{(p)}, x_2)$$

Denotemos por $\mathcal{J}$ a esta última *fbf*. En este punto servirá de ayuda el dar una interpretación grosera de $\mathcal{J}$, a fin de comprender su significado. En primer lugar, W es la interpretación de $\mathcal{W}$. Por tanto, $\mathcal{J}$ puede interpretarse como:

«Para todo $n \in D_N$, $W(p, n)$ no se verifica.»

Desarrollando esto, resulta:

«Para todo $n \in D_N$, no es cierto que p sea el número de Gödel de una *fbf* $\mathcal{A}(x_1)$ en la que x_1 aparece libre, y que n sea el número de Gödel de una demostración de $\mathcal{A}(0^{(p)})$ en $\mathcal{N}$.»

Ahora bien, p es el número de Gödel de una *fbf* en la que aparece libre x_1, a saber, la *fbf* $(\forall x_2) \sim \mathcal{W}(x_1, x_2)$, y si denotamos a esta *fbf* por $\mathcal{A}(x_1)$, entonces $\mathcal{A}(0^{(p)})$ es la *fbf* $\mathcal{J}$. Así pues, la interpretación de la *fbf* $\mathcal{J}$ equivale a:

«Para todo $n \in D_N$, n no es el número de Gödel de una demostración de la *fbf* $\mathcal{J}$ en $\mathcal{N}$.»

Así pues, en un cierto sentido puede considerarse que la *fbf* $\mathcal{J}$ afirma su propia indemostrabilidad.

Si $\mathcal{N}$ no fuese consistente sería trivialmente completo, ya que toda *fbf* sería un teorema. El teorema de incompletitud requerirá, pues, la hipótesis de que $\mathcal{N}$ es consistente. De hecho, la demostración de Gödel requería una hipótesis ligeramente más fuerte, que hemos de investigar ahora.

Definición 6.30

Un sistema de primer orden S con el mismo lenguaje que $\mathcal{N}$ es *ω-consistente* si para ninguna *fbf* $\mathcal{A}(x_1)$ en la que aparezca libre x_1 se tiene que $\sim(\forall x_1)\mathcal{A}(x_1)$ es un teorema de S, supuesto que $\mathcal{A}(0^{(n)})$ sea un teorema de S para todo $n \in D_N$.

Como hemos observado ya anteriormente (véase Observación 6.6), si $\mathcal{A}(0^{(n)})$ es un teorema para todo n, $(\forall x_1)\mathcal{A}(x_1)$ no ha de ser necesariamente un teorema. La ω-consistencia asegura que si cada $\mathcal{A}(0^{(n)})$ es un teorema, entonces $\sim(\forall x_1)\mathcal{A}(x_1)$ *no es* un teorema, independientemente de si $(\forall x_1)\mathcal{A}(x_1)$ es o no un teorema.

Proposición 6.31

Sea S un sistema de primer orden con el mismo lenguaje que $\mathcal{N}$. Si S es ω-consistente, entonces S es consistente.

Demostración: Sea $\mathcal{A}(x_1)$ cualquier *fbf.* tal que $\mathcal{A}(0^{(n)})$ sea un teorema

de S para todo n. Por ejemplo, $\mathscr{A}(x_1)$ podría ser $x_1 = x_1$. Entonces, por la ω-consistencia $\sim(\forall x_1)\mathscr{A}(x_1)$ no es un teorema de S. Así pues, S es consistente (pues existe una *fbf* que no es un teorema).

Proposición 6.32 (Teorema de Incompletud de Gödel)

Bajo la hipótesis de que $\mathscr{N}$ sea ω-consistente, la *fbf* $\mathscr{J}$ no es un teorema de $\mathscr{N}$, ni tampoco lo es su negación. Por tanto, si $\mathscr{N}$ es ω-consistente, entonces $\mathscr{N}$ no es completo.

Demostración: Supongamos primero que $\mathscr{J}$ es un teorema de $\mathscr{N}$, y sea q el número de Gödel de una demostración de $\mathscr{J}$ en $\mathscr{N}$. Al igual que antes, sea p el número de Gödel de $(\forall x_2)\sim\mathscr{W}(x_1, x_2)$. Entonces se verifica $W(p, q)$. W es expresable en $\mathscr{N}$ mediante $\mathscr{W}$, así que tenemos

$$\vdash_{\mathscr{N}} \mathscr{W}(0^{(p)}, 0^{(q)}).$$

Pero $\vdash_{\mathscr{N}} \mathscr{J}$, es decir, $\vdash_{\mathscr{N}} (\forall x_2)\sim\mathscr{W}(0^{(p)}, x_2)$, y con ello $\vdash_{\mathscr{N}} \sim\mathscr{W}(0^{(p)}, 0^{(q)})$, usando $(K5)$ y MP. Esto contradice la consistencia de $\mathscr{N}$, de modo que $\mathscr{J}$ no puede ser un teorema de $\mathscr{N}$.

$\mathscr{J}$ no es un teorema de $\mathscr{N}$; es decir, no existe demostración de $\mathscr{J}$ en $\mathscr{N}$, de modo que ningún número q es el número de Gödel de una demostración de $\mathscr{J}$, es decir, de $(\forall x_2)\sim\mathscr{W}(0^{(p)}, x_2)$, en $\mathscr{N}$. Así pues, $W(p, q)$ no se verifica para ningún número q. Por tanto

$$\vdash_{\mathscr{N}} \sim\mathscr{W}(0^{(p)}, 0^{(q)}) \text{ para todo } q.$$

Por la ω-consistencia se tiene entonces que

$$\sim(\forall x_2)\sim\mathscr{W}(0^{(p)}, x_2)$$

no es un teorema de $\mathscr{N}$, es decir, $(\sim\mathscr{J})$ no es un teorema de $\mathscr{N}$.

Observación 6.33

Hemos explicitado la hipótesis de la ω-consistencia, a pesar de que existe una demostración obvia de que $\mathscr{N}$ es ω-consistente, usando el modelo N. No obstante, como ya hemos mencionado anteriormente, los argumentos que hacen uso de modelos tienden a involucrar hipótesis que a menudo se refieren a la consistencia de otros sistemas formales, tendiéndose así a desplazar el problema. Además, la Proposición 6.32 puede generalizarse a otros sistemas formales que son extensión de $\mathscr{N}$, y en estos casos ha de hacerse ciertamente la hipótesis de la ω-consistencia, a falta de otra información específica.

▷ Hasta aquí, este capítulo ha sido una versión esbozada de la demostración del Teorema de Incompletitud de Gödel. Se ha incluido para

dar idea de los métodos involucrados y facilitar alguna explicación de su importancia. Examinemos, pues, algunas consecuencias y generalizaciones.

Proposición 6.34 (Suponiendo que $\mathcal{N}$ sea ω-consistente)

$\mathcal{N}$ contiene una *fbf* cerrada que es verdadera en el modelo N pero no es un teorema de $\mathcal{N}$.

Demostración: La *fbf* $\mathcal{J}$ es cerrada. Ni $\mathcal{J}$ ni $(\sim\mathcal{J})$ son teoremas de $\mathcal{N}$. Sin embargo, o $\mathcal{J}$ es verdadera en N o $(\sim\mathcal{J})$ es verdadera en N, ya que N es una interpretación.

▷ De hecho, la hipótesis de la proposición anterior puede debilitarse.

Proposición 6.35 (Suponiendo que $\mathcal{N}$ sea consistente)

$\mathcal{N}$ contiene una *fbf* cerrada que es verdadera en el modelo N pero no es un teorema de $\mathcal{N}$.

Demostración: Hay que hacer modificaciones en la demostración de la Proposición 6.32, que sigue valiendo con la hipótesis debilitada; pero hay que modificar también la *fbf* $\mathcal{J}$. Omitimos detalles.

▷ $\mathcal{N}$ no es completo. Nuestro primer pensamiento podría ser ahora: ¿Cómo podemos completar $\mathcal{N}$? Quizá hemos escogido para $\mathcal{N}$ un conjunto de axiomas inadecuado. Quizá si añadiésemos la *fbf* $\mathcal{J}$ como nuevo axioma el nuevo sistema sería completo. Una pequeña reflexión acerca de los procedimientos involucrados en este capítulo nos indicará que el añadir $\mathcal{J}$ como nuevo axioma no ayuda. Sea $\mathcal{N}^+$ el sistema obtenido a partir de $\mathcal{N}$ introduciendo $\mathcal{J}$ entre los axiomas. Este cambio en los axiomas no afecta al resultado de que toda relación recursiva es expresable (aunque podría afectar al recíproco). Sin embargo, la recursividad de las relaciones *Prax*, *Dm* y otras definidas en términos de éstas podría verse afectada. Pero la adición de un solo axioma no afecta a la recursividad del conjunto de números de Gödel de los axiomas, ya que todo conjunto unitario es recursivo y la unión de dos conjuntos recursivos es recursivo. La relación *Prax* permanece, pues, recursiva, y de modo similar puede verse que *Dm* y otras, incluyendo *W*, son recursivas pese a que sus definiciones se refieren, naturalmente, a $\mathcal{N}^+$ en lugar de a $\mathcal{N}$. Puede llevarse a cabo el mismo desarrollo que para $\mathcal{N}$, lo que lleva a un teorema de incompletitud que involucra otra $\mathcal{J}'$ diferente.

Mediante una argumentación más general en esta misma línea, obtenemos la siguiente proposición.

Proposición 6.36

Sea S una extensión cualquiera de $\mathcal{N}$ tal que el conjunto de los números de Gödel de los axiomas propios de S sea recursivo. Entonces (supuesto S consistente) S no es completo.

Observación 6.37

La hipótesis hecha acerca de S equivale a suponer que la relación $Prax_S$ definida por: $Prax_S(n)$ se verifica si y sólo si n es el número de Gödel de un axioma propio de S, es recursiva. Es esta hipótesis la que permite demostrar para S una proposición correspondiente a la Proposición 6.29.

▷ De esta última proposición se deduce que $\mathcal{N}$ no puede completarse añadiendo un conjunto de axiomas adicionales cuyos números de Gödel constituyen un conjunto finito o infinito recursivo.

Como ya hemos hecho notar, el sistema $\mathcal{N}$ es deficiente en un sentido particular: Sus axiomas incluyen solamente una versión débil del Principio de Inducción Matemática. Esto se debe al uso de un lenguaje de primer orden. ¿Podríamos evitar la dificultad de la incompletitud considerando un sistema de segundo orden de la aritmética? En este libro hemos eludido deliberadamente la complicación adicional involucrada en los sistemas de segundo orden, de modo que toda investigación de esta cuestión queda fuera de nuestro alcance. Se sabe, no obstante, que la aritmética de segundo orden tiene la misma propiedad, es decir, un sistema aritmético de segundo orden en el que el conjunto de (los números de Gödel de) los axiomas propios sea recursivo, no es completo.

Las consecuencias del teorema de Gödel son todavía de mayor alcance. Hemos visto que el sistema de los números naturales puede definirse dentro de ZF. Todo sistema formal de teoría de conjuntos, si es adecuado para ella, compartirá esta propiedad, y de hecho algunos sistemas más restringidos que ZF la compartirán también. (Un ejemplo de sistema que *no* la comparte es nuestro sistema formal de teoría de grupos, que es demasiado restringido.)

Proposición 6.38

Todo sistema de primer orden suficientemente fuerte, cuyo conjunto de (números de Gödel de) axiomas propios sea recursivo, y que sea consistente, no es completo. (Un sistema es suficientemente fuerte si el sistema de los números naturales puede definirse en él del modo antes visto, de modo que los axiomas de la aritmética pasen a ser teoremas.) En particular, si ZF es consistente, entonces no es completo.

▷ Finalmente, consideremos lo que el lector atento habrá advertido ya, a saber, que existe una extensión completa de $\mathcal{N}$. Las hipótesis del Teorema de Incompletitud de Gödel incluyen el requerimiento de que el sistema formal en cuestión tenga un conjunto de axiomas propios cuyos números de Gödel constituyan un conjunto recursivo. Esta era una hipótesis necesaria para la demostración, ya que ésta involucraba demostraciones de que ciertas relaciones eran también recursivas. El hecho de que exista un sistema de primer orden consistente y completo, y que, por tanto, no satisface este requerimiento, puede verse utilizando un procedimiento dado en el Capítulo 4 del modo siguiente.

Consideremos la extensión de $\mathcal{N}$ obtenida añadiendo como axiomas todas las *fbfs* de $\mathcal{N}$ verdaderas en el modelo N. Esta extensión es completa y consistente, supuesto que $\mathcal{N}$ sea consistente (véase el Corolario 4.47). Por la Proposición 6.36, se tiene entonces que el conjunto de axiomas propios de esta extensión puede ser recursivo. De esto se deduce que el conjunto de los números de Gödel de las *fbfs* de $\mathcal{N}$ que son verdaderas en $\mathcal{N}$ es un ejemplo de conjunto no recursivo.

Por lo tanto, si admitimos conjuntos de axiomas propios no recursivos, puede tenerse un sistema de primer orden para la aritmética que sea consistente y completo. El problema que esto plantea es el siguiente: ¿Qué tienen los conjuntos recursivos que haga que valga la pena considerar el resultado del Teorema de Incompletitud de Gödel como significativo? No puede decirse con verdad que ningún sistema formal consistente para la aritmética es completo. Todo lo que puede decirse es que ningún sistema así cuyo conjunto de (números de Gödel de) axiomas sea recursivo es completo. La respuesta se encuentra en las ideas de computabilidad, efectividad y algoritmo, y en su relación con la idea de recursividad. De estas ideas trataremos en el siguiente capítulo.

Ejercicio

18 Supóngase la *fbf* $\mathcal{J}$ definida como en el texto. $\mathcal{J}$ no es un teorema de $\mathcal{N}$, así que la extensión de $\mathcal{N}$ obtenida añadiendo $(\sim\mathcal{J})$ como axioma adicional es consistente (supuesto que $\mathcal{N}$ sea consistente). Demuéstrese que esta extensión no es ω-consistente.

7
Computabilidad Insolubilidad Indecidibilidad

7.1 Algoritmo y computabilidad

En un congreso mundial de matemáticos del año 1900, Hilbert presentó su célebre lista de problemas matemáticos no resueltos sobresalientes. Uno de ellos (conocido ahora como el décimo problema de Hilbert) era el problema de encontrar un procedimiento para decidir si una ecuación diofántica polinómica arbitrariamente dada tiene solución entera. La solución al problema (no encontrada hasta muy recientemente —véase Davis 1—) se presentó en términos que hubiesen sorprendido al auditorio de Hilbert de 1900 (y posiblemente al propio Hilbert), ya que no consiste en un conjunto de instrucciones que definan el procedimiento requerido, sino más bien en una demostración de que dicho procedimiento no puede existir. El décimo problema de Hilbert es un ejemplo de lo que hoy día se llama popularmente «problema insoluble», o, para ser más exactos, un problema recursivamente insoluble. Investigaciones acerca de este problema y de otros como él llevaron a los matemáticos de principios de siglo a considerar lo que significa la palabra «procedimiento» según lo requiere el problema. Estas consideraciones llevaron a las ideas y aplicaciones descritas en este capítulo.

En este contexto, otra palabra con el mismo significado que «procedimiento» es la palabra «algoritmo», y normalmente usaremos esta última debido a que la primera tiene otros significados fuera de este contexto, que podrían llevar a confusión. La noción de algoritmo es una noción intuitiva y no una noción matemáticamente precisa —intentaremos definirla del modo siguiente.

Definición 7.1

Un *algoritmo* es un conjunto de instrucciones efectivo y explícito, para un procedimiento de cómputo (no necesariamente numérico) que puede

usarse para encontrar la respuesta de cualquier pregunta de entre las de una clase determinada.

Puesta la definición en estos términos, surgen de manera natural cuestiones referentes a la existencia de algoritmos apropiados para diferentes «clases de preguntas». En el décimo problema de Hilbert la clase de preguntas es

{¿existe una solución entera de la ecuación E?/
E ecuación diofántica polinómica}.

Ejemplo 7.2

Puede considerarse clases de preguntas de cualquier tipo, por ejemplo,

(*a*) {¿cuál es el valor de $f(n)$? $/n \in D_N$} (f función fija).
(*b*) {¿es n miembro del conjunto A? $/n \in D_N$} (A conjunto fijo).
(*c*) {¿es $\mathscr{A}$ un teorema de $\mathscr{N}$? $/\mathscr{A}$ *fbf* de $\mathscr{N}$}.

Ejemplo 7.3

(*a*) {¿Es 2 factor de n? $/n \in D_N$}.

Existe un algoritmo que proporciona respuestas a esta clase de preguntas. Dado cualquier número n, hállese el resto de la división por 2 (usando cualquiera de los conocidos procedimientos «escolares» de división). Si el resto es 0, dése la respuesta sí. Si el resto es 1, dése la respuesta no.

(*b*) {¿Pertenece n al conjunto de los números primos? $/n \in D_N$}.

Existe un algoritmo que proporciona respuestas a esta clase de preguntas. Dado cualquier número n, hay métodos standard para hallar el resto de la división de n entre m, para todo m $(1 < m < n)$. Si ninguno de estos restos es cero, entonces n es un número primo. Si uno o más de estos restos es cero, entonces n no es un número primo.

(*c*) {¿Cuál es el valor de $f(n)$? $/n \in D_N$}, siendo f la función definida por $f(n) = 2n$ $(n \in D_N)$.

En este caso, la aritmética escolar elemental vuelve a proporcionar un algoritmo para calcular los valores de f.

(*d*) {¿Cuáles son las soluciones complejas de la ecuación E? /E ecuación cuadrática con coeficientes enteros}.

Existe una fórmula algebraica bien conocida que proporciona un algoritmo para este caso.

▷ Se habrá notado que «clase de preguntas» es una noción muy general en este contexto. Restrinjámonos por el momento a la consideración de algoritmos en relación con clases de preguntas de una naturaleza particular; concretamente, la ejemplificada por el Ejemplo 7.3(*c*) de

más arriba. En otras palabras, consideremos la noción de «función computable mediante algoritmo». Siguiendo la historia del desarrollo de la materia este aspecto fue el que recibió atención más tempranamente. Se hicieron intentos independientes por parte de varios investigadores para hacer matemáticamente precisa la noción de algoritmo y caracterizar matemáticamente la clase de las funciones computables mediante un algoritmo. Naturalmente, el si una cierta descripción matemática particular de la noción de algoritmo corresponde exactamente a la idea intuitiva no es algo que pueda demostrarse. No obstante, como veremos, hay buenas razones para suponer que una cierta descripción matemática del concepto de algoritmo es lo bastante general como para incluir todos los algoritmos intuitivos.

Las descripciones dadas por los primeros investigadores tomaron diferentes formas, que pueden caracterizarse burdamente del siguiente modo:

(*a*) máquinas computadoras abstractas (definidas de modo preciso),

(*b*) construcciones formales de procedimientos de cómputo,

y

(*c*) construcciones formales productoras de clases de funciones.

Las dos primeras caracterizaciones se refieren a la propia noción de algoritmo (en principio no hay diferencia entre (*a*) y (*b*)). La última da descripciones de la clase de funciones computables mediante un algoritmo.

Un ejemplo de (*a*) son las *máquinas de Turing*, que fueron diseñadas por Turing en los años 30. La idea es la de una máquina ideal que procesa una cinta ideal sobre la que está impreso el número (o números) de entrada en forma codificada, siguiendo ciertas reglas predeterminadas de naturaleza sencilla y restringida, y produce sobre la cinta al final del cálculo el resultado de salida de forma similar, codificada. Se pretende que todo algoritmo destinado a computar los valores de una función pueda trasladarse a instrucciones para una tal máquina.

Un ejemplo de (*b*) son los *sistemas de Thue*, que son sistemas puramente formales en los que pueden «deducirse» sucesiones finitas de símbolos como consecuencia de otras sucesiones finitas de símbolos por medio de ciertas reglas. Así pues, dada una sucesión finita de símbolos como entrada, las reglas permiten convertirla en una sucesión finita de salida. (Véase Davis [2].)

Un ejemplo de (*c*) lo proporcionan las funciones recursivas. Las funciones básicas y las reglas son una construcción formal para generar una clase de funciones.

Todas estas construcciones tienen en común una cosa: el incluir funciones parciales. Es razonable decir que una función parcial es com-

putable mediante un algoritmo si existe un algoritmo que arroja el valor de la función cuando ésta está definida. En el contexto de las máquinas de Turing esto corresponde a permitir que las reglas de una máquina lleven a un cómputo que nunca finalice, no dando así lugar a ningún resultado de salida. En el contexto de las funciones recursivas, esto corresponde a permitir el uso del operador de minimización sin restricciones, como se indicó en la Observación 6.13.

El resultado crucial es que las diversas caracterizaciones de las funciones (parciales) computables mediante un algoritmo condujeron todas a una misma clase, a saber, la clase de las funciones parciales recursivas +. Esto es algo susceptible de demostración, y que ha sido demostrado. Lo que no es susceptible de demostración es si la clase de las funciones parciales recursivas coincide con la clase de las funciones computables mediante un algoritmo. No obstante, a la luz de la evidencia a favor y de la falta de evidencia en contra, aceptamos la *Tesis de Church* que afirma:

> La clase de las funciones parciales computables mediante un algoritmo es idéntica a la clase de las funciones parciales recursivas.

Observación 7.4

El aceptar la Tesis de Church no supone más que cristalizar nuestra idea intuitiva de algoritmo de modo que corresponda con las descripciones matemáticas que hemos dado. No hay ninguna evidencia de que hacer esto no sea una cosa razonable.

▷ Ahora, bajo la hipótesis de la Tesis de Church, los problemas referentes a existencia de algoritmos se hacen más manejables matemáticamente. Por ejemplo, el problema de si existe un algoritmo que proporcione los valores de una función particular se convierte en el problema de si esa función es recursiva. En otro contexto, el problema de si existe un algoritmo que decida acerca de la pertenencia a un subconjunto dado de D_N se convierte en el problema de si la función característica de dicho conjunto es recursiva, es decir, de si el conjunto es recursivo.

La utilidad de la Tesis de Church radica en el hecho de que pueden usarse técnicas matemáticas para demostrar que una función o un conjunto dado es (o no es) recursivo, y con ello, para demostrar que existe (o no existe) un algoritmo para una clase particular de problemas. Y, recíprocamente, es a menudo útil el deducir, habiendo encon-

---

+ El término standard en la literatura es «función recursiva parcial» más que «función parcial recursiva», pero aquí usamos este último por razones de claridad.

trado un algoritmo particular, que el conjunto o función correspondiente es recursivo.

El lector notará quizá que una de las mitades de la Tesis de Church tiene más contenido que la otra. La Tesis de Church equivale a la conjunción de:

(i) Toda función parcial computable mediante un algoritmo es una función parcial recursiva,

e

(ii) Toda función parcial recursiva es computable mediante un algoritmo.

La segunda de estas aseveraciones puede someterse a demostración, ya que puede darse una «demostración» inductiva de ella usando una noción intuitiva razonable de algoritmo. Para ello se describen algoritmos que calculan cada una de las funciones recursivas básicas (paso base de la inducción), y se demuestra cómo pueden usarse algoritmos que calculen ciertas funciones para construir algoritmos que calculen las funciones obtenidas a partir de éstas por medio de las reglas I, II y III.

La primera de las aseveraciones de más arriba es la parte de la Tesis de Church que no puede ser demostrada. Lo que se ha demostrado es que, para un cierto número de definiciones matemáticas precisas diferentes de la noción de algoritmo, todas las funciones parciales computables mediante esa clase de algoritmos son recursivas.

A partir de todo esto puede verse que, si se han de usar técnicas de recursividad en la discusión de la existencia de algoritmos para ciertas clases particulares de problemas, la Tesis de Church será vital, si la respuesta ha de ser que no existe ningún algoritmo. A partir de la conclusión de que una función o conjunto particular no es recursivo, sólo podemos deducir que no existe ningún algoritmo asumiendo la Tesis de Church.

Ejemplo 7.5

(*a*) Sean f y g funciones de un argumento sobre D_N, computables mediante algoritmo. Entonces fog es computable mediante algoritmo. Puesto que para calcular $fog(n)$, basta con calcular $g(n)$ usando el algoritmo para g y calcular seguidamente $f(g(n))$ usando el algoritmo para f. Esto puede generalizarse fácilmente, de modo que cubra la aplicación de la regla II para la construcción de funciones recursivas.

(*b*) Sea f: $D_N \rightarrow D_N$ definida por recursión a partir de la función g, es decir

$$f(0) = k$$
$$f(n+1) = g(n, f(n)).$$

Supongamos que g es computable mediante un algoritmo. Indicamos un algoritmo para calcular $f(m)$, para todo $m \in D_N$. Si $m=0$ entonces $f(m)=k$. Si $m>0$, calculamos $f(1)=g(0, f(0))$ usando el algoritmo para g, después $f(2)=g(1, f(1))$ usando el algoritmo para g, y así sucesivamente, hasta obtener el valor de $f(m)$.

(*c*) Un caso más específico de (*b*) es la función factorial: $f(n)=n!$ ($n \in D_N$). Para calcular 10!, por ejemplo, lo que hacemos en la práctica es calcular el procedimiento dado en (*b*), calculando sucesivamente 1!, 2!, 3!, ..., 9!, 10!.

(*d*) Consideremos la función h: $D_N \to D_N$ dada por $h(n)=$el primer dígito no nulo del desarrollo decimal de $1/n$. Es posible demostrar que h es recursiva directamente a partir de la definición, pero el procedimiento sería bastante complejo. Alternativamente, podemos describir un algoritmo que podría usarse para calcular los valores de la función, y deducir entonces, usando la Tesis de Church, que h es recursiva. El algoritmo se basa en el procedimiento standard de división: Primero se encuentra el menor valor de k tal que $n<10^k$, y después se halla el cociente de la división de 10^k entre n.

(*e*) Sabemos que el conjunto de los números de Gödel de las *fbfs.* de $\mathcal{N}$ que son verdaderas en N no es recursivo. Se deduce entonces de la Tesis de Church que no existe ningún algoritmo que responda a preguntas de la clase

$$\{\text{¿es } \mathscr{A} \text{ verdadera en } N?/\mathscr{A} \textit{ fbf} \text{ de } \mathcal{N}\}$$

(*f*) Sea A el subconjunto de D_N que consta de todos los números que son suma de dos cuadrados. A es recursivo, pero sería bastante difícil demostrar directamente que la función f: $D_N \to D_N$ dada por

$$f(n)=\begin{cases}0 \text{ si existen } p, q \in D_N \text{ tales que } n=p^2+q^2\\ 1 \text{ en otro caso}\end{cases}$$

es recursiva. No obstante, existe un algoritmo que responde a preguntas de la clase $\{¿n \in A?/n \in D_N\}$. Podemos describirlo como sigue: Dado n, calcúlese p^2+q^2 para todo par de números p, q, ambos menores que n. Si para algún par p, q resulta $p^2+q^2=n$, contéstese «sí». Si para ningún par p, q se tiene $p^2+q^2=n$, contéstese «no». Por la Tesis de Church se tiene entonces que A es un conjunto recursivo.

▷ ¿Qué relevancia tiene todo esto con respecto a la hipótesis hecha en la Proposición 6.36 de que el conjunto de los números de Gödel de los axiomas propios debe ser recursivo? A la luz de la Tesis de Church, para todo sistema S que tenga esta propiedad existirá un algoritmo que responderá a preguntas del conjunto

$$\{\text{¿es } \mathscr{A} \text{ un axioma propio de } S?/\mathscr{A} \textit{ fbf} \text{ de } S\}$$

Más aún: Para un sistema S que no tenga esta propiedad no existirá un tal algoritmo.

Desde el punto de vista que tomamos al introducir la idea de sistema formal, es decir, el intento de usar sistemas formales para reflejar auténticos contextos matemáticos y hacerlos precisos, podemos ver que un sistema S para el cual no exista ningún algoritmo para decidir si una *fbf* de S es un axioma de S, no es satisfactorio. No servirá de ayuda para decidir qué enunciados del contexto matemático son verdaderos, pues no habrá ningún procedimiento efectivo para decidir qué enunciados corresponden a *fbfs* que son axiomas, ni tampoco habrá ningún procedimiento efectivo para decidir si una sucesión finita dada de *fbfs* es una demostración. Uno de los propósitos del estudio inicial de los sistemas formales era el buscar un procedimiento formal que decidiese si un enunciado matemático cualquiera es verdadero, incluyendo entre las *fbfs* demostrables tantas *fbfs* verdaderas como fuese posible. Un sistema formal en el que el conjunto de axiomas no sea recursivo no puede usarse para esto. Un sistema formal cuyo conjunto de axiomas sea recursivo ciertamente se ajusta a los requerimientos precisos para que existan procedimientos efectivos para decidir lo que es un axioma y lo que es una demostración. No obstante, el teorema de incompletud nos dice que ni siquiera un sistema así (para la aritmética) es útil, ya que el conjunto de teoremas del sistema no incluye todas las *fbfs* verdaderas (en la interpretación N).

Observación 7.6

El lector puede cuidarse de considerar el sistema $\mathcal{N}$, en el cual el conjunto de (los números de Gödel de) los axiomas propios es recursivo, y diseñar un procedimiento efectivo con cuya ayuda pueda enumerarse el conjunto de los teoremas de $\mathcal{N}$. (Indicación: La relación *Dm* sobre pares de números de Gödel es recursiva, y por lo tanto existe un algoritmo para decidir si un par dado la verifica.) Esto muestra que el conjunto de (números de Gödel de) teoremas de $\mathcal{N}$ es «efectivamente enumerable». Esto nos lleva a una nueva noción.

Definición 7.7

Un subconjunto de D_N es *recursivamente enumerable* si es el rango de una función recursiva, o si es vacío.

Un conjunto es recursivamente enumerable si existe una función recursiva f tal que $f(0), f(1), f(2), \ldots$ es una lista de todos los elementos del conjunto (eventualmente con repeticiones). La Tesis de Church implica que «recursivamente enumerable» es equivalente a «efectivamente enumerable».

▷La pregunta que podemos hacer inmediatamente es: ¿Son «recursivo» y «recursivamente enumerable» nociones distintas? ¿Existe algún conjunto que sea recursivamente enumerable, pero no recursivo, o viceversa? La siguiente demostración de una respuesta parcial a esta pregunta es una buena ilustración del uso que puede hacerse de la Tesis de Church.

Proposición 7.8

Todo conjunto recursivo es recursivamente enumerable.

Demostración: Sea A un conjunto recursivo, de modo que su función característica C_A es computable mediante un algoritmo. Vamos a describir un algoritmo que enumera los miembros de A. Se calculan por turno los valores $C_A(0)$, $C_A(1)$, ... y se hace una lista de todos los números n tales que $C_A(n)=0$. Por la Tesis de Church se tiene entonces que, por ser A efectivamente enumerable, A es recursivamente enumerable.

▷La recíproca de esta proposición es falsa. Existen varias demostraciones de esto, puesto que todo lo que necesitamos es un contraejemplo. Proporcionamos uno demostrando un resultado importante acerca del sistema $\mathcal{N}$.

Definición 7.9

Un sistema formal es *recursivamente indecidible* si el conjunto de los números de Gödel de los teoremas del sistema no es recursivo.

Nótese que, usando la tesis de Church, se tiene que un sistema formal S es recursivamente indecidible si y sólo si no existe ningún algoritmo que responde a preguntas del conjunto

$$\{\text{¿es } \mathscr{A} \text{ un teorema?}/\mathscr{A} \textit{ fbf} \text{ de } S\}$$

▷Más tarde demostraremos que $\mathcal{N}$ es recursivamente indecidible, después de algún trabajo preliminar. La Observación 7.6, junto con la Tesis de Church, indica que el conjunto de los (números de Gödel de los) teoremas de $\mathcal{N}$ es recursivamente enumerable. La indecibilidad recursiva de $\mathcal{N}$ demuestra que este conjunto no es recursivo.

Corolario 7.10

Existe un subconjunto de D_N que es recursivamente enumerable pero no recursivo.

▷La última parte de este capítulo va a referirse a la indecibilidad recursiva y a la noción más general de insolubilidad recursiva. Ya tenemos una idea de lo que es esta última noción, pero vamos a precisarla, a efectos de futuras referencias.

Definición 7.11

Una clase de preguntas es *recursivamente insoluble* si no existe ningún

algoritmo que proporcione respuesta a todas las preguntas de la clase. (Nótese la asunción de la Tesis de Church que va implícita en el uso de la palabra «recursivamente» en esta definición).

Así pues, un sistema formal S es recursivamente indecidible si y sólo si la clase de preguntas

$$\{\text{¿es } \mathscr{A} \text{ un teorema de } S?/\mathscr{A} \textit{ fbf} \text{ de } S\}$$

es recursivamente insoluble.

Ejercicios

1 Descríbanse algoritmos que proporcionen respuestas para las siguientes clases de preguntas:
   (*a*) {¿es n el número de Gödel de un término de $\mathscr{N}?/n \in D_N$}.
   (*b*) {¿cuál es el máximo común divisor de m y $n?/m, n \in D_N$}.
   (*c*) {¿es n un cuadrado perfecto?/$n \in D_N$}.
   (*d*) {¿es $\mathscr{A}$ consecuencia en L del conjunto $\Gamma?/\mathscr{A}$ *fbf* de L} (Γ conjunto finito fijo de *fbfs* de L).
   (*e*) {¿cuál es la derivada de la función $f?/f$ función polinómica de una variable real}.
   (*f*) {¿cuál es el n-ésimo número primo impar?/$n \in D_N$}.
2 Demuéstrese para todo subconjunto A de D_N, si A y sus complementarios son recursivamente enumerables, entonces A es recursivo. (Indicación: Usese la Tesis de Church). Dedúzcase que existe un subconjunto de D_N que no es ni recursivo ni recursivamente enumerable.
3 Demuéstrese que si un conjunto infinito A es recursivamente enumerable en orden creciente (es decir, si existe una función recursiva f tal que $f(0), f(1), f(2), \ldots$ sea una lista de los miembros de A y $f(n) < f(n+1)$ para todo $n \geqslant 0$), entonces A es recursivo.
4 Demuéstrese que las siguientes funciones son recursivas:
   (*a*) φ, siendo $\varphi(n) =$ el número de enteros positivos p menores que n tales que p y n no tienen factores comunes ($n \in D_N$).
   (*b*) f, siendo $f(m, n) =$ mínimo entero mayor que m/n ($m, n \in D_N$).
   (*c*) g, siendo

$$g(n) = \begin{cases} 0 & \text{si existe una sucesión de al menos } n \text{ 7}s \text{ consecutivos} \\ & \text{en el desarrollo decimal de } \pi. \\ 1 & \text{en otro caso.} \end{cases}$$

   (*d*) q, siendo

$$q(m, n) = \begin{cases} & \text{el número de Gödel de } (\mathscr{A} \to \mathscr{B}) \text{ si } m \text{ y } n \text{ son los números} \\ & \text{de Gödel de las } \textit{fbfs}. \ \mathscr{A} \text{ y } \mathscr{B} \text{ de } \mathscr{N}. \\ 0 & \text{en otro caso } (m, n \in D_N). \end{cases}$$

5 Dense ejemplos de
   (*a*) Un conjunto recursivo que posea un subconjunto no recursivo.
   (*b*) Un conjunto no recursivo que posea un subconjunto recursivo infinito.
6 Demuéstrese que todo conjunto recursivamente enumerable infinito posee un subconjunto recursivo infinito.

7.2 Máquinas de Turing

Es un ejercicio valioso el entrar en los detalles de una de las caracterizaciones computacionales de la noción de algoritmo. La caracterización de Turing es la más útil y la más sencilla de entender, y puede aplicarse directamente como veremos, a problemas de decidibilidad y solubilidad.

El lector debe dejarse confundir por el uso de la palabra «máquina». Las máquinas de Turing no son máquinas calculadoras reales, sino sistemas abstractos, definidos con precisión de una manera matemática de modo que reflejen procedimientos de cálculo. La terminología que usaremos indica claramente que la «máquina» funciona, y es cierto de hecho que pueden construirse máquinas reales que siguen los procedimientos de una máquina de Turing «notacional».

El propósito de Turing al describir sus máquinas era reducir los cómputos a sus rasgos esenciales más escuetos, describiendo de un modo sencillo algunos procedimientos básicos que son manifiestamente efectivos y a los que pueda reducirse cualquier procedimiento efectivo. Examinemos ahora los detalles técnicos.

Una máquina de Turing puede imaginarse como una caja negra a través de la cual pasa una cinta de papel, dividida en cuadros iguales que pueden o no llevar un símbolo impreso sobre ellos. Para un cierto cómputo particular, la máquina comenzará con una cantidad finita de información de entrada sobre la cinta, es decir, con símbolos impresos tan sólo sobre un número finito de cuadros. La máquina procesa la cinta de acuerdo con ciertas reglas, y eventualmente puede llegar a detenerse. Si se detiene, la información de salida es lo que queda sobre la cinta. Si no se detiene, el cómputo es indeterminado y no hay salida.

Antes de proseguir, detengámonos en dos de los puntos tocados más arriba, que requieren comentario. El requerimiento de que la información de entrada sea finita parece ciertamente razonable. De hecho, el lector quizá se admire de que sea necesario enunciarlo, puesto que toda cinta de papel existente es ciertamente de longitud finita y sólo puede consistir en un número finito de cuadros iguales. No obstante, sería razonable imponer una cota definida a la longitud de cinta requerida para la información de entrada. Además, mientras la máquina procesa la cinta puede llegar a necesitar más «espacio de trabajo» del que proporciona la cinta de entrada original, por lo que consideraremos la cinta como extensible indefinidamente. Cada cómputo requerirá tan sólo una cantidad finita de cinta, pero no sería razonable poner una cota absoluta a la longitud finita de cinta disponible, así que diremos que la cinta es *potencialmente infinita.*

Además de no imponer cotas a la cinta, no impondremos cota al

tiempo que la máquina requiere para un cómputo. En un computador real nos veíamos forzados a imponer un límite de tiempo, y en caso de que no se produjese respuesta en ese tiempo, tendríamos que darnos por vencidos y tratar de encontrar un programa diferente que redujese el tiempo requerido. No obstante, para nuestras máquinas abstractas sería una restricción artificial el poner un límite absoluto al número de pasos o al tiempo requerido para obtener una respuesta. Todo lo que requerimos es que, si hay respuesta, la máquina la produzca en un tiempo finito y después de un número finito de pasos. Así pues, en el curso de un cómputo podemos no saber (y en general no sabremos) si el cómputo terminará o no.

Con el fin de estudiar lo que este tipo de máquinas pueden hacer es necesario especificar tanto la naturaleza de la información simbólica que puede aparecer sobre la cinta como las maneras en que la máquina puede procesarla.

Una máquina de Turing tiene un *alfabeto de símbolos para la cinta* que puede variar de máquina a máquina, pero que no es más que una lista finita de símbolos. Cada cuadro de la cinta puede tener impreso sobre él a lo sumo uno de estos símbolos a un tiempo. Generalmente se incluye en la lista de símbolos la letra *B*, que denotará un cuadro en blanco. La máquina de Turing más sencilla no tendrá más que dos símbolos para la cinta, *B* y, pongamos, 1.

La máquina de Turing opera del modo siguiente: En cualquier momento dado la máquina está «leyendo» un único cuadro de la cinta. Puede reemplazar el símbolo que aparezca en este cuadro (si lo hay) por otro símbolo, o imprimir un símbolo sobre él si el cuadro está en blanco, o dejar el cuadro inalterado, en cuyo caso podrá desplazar su atención al cuadro siguiente a la derecha o a la izquierda sobre la cinta. Tenemos pues:

Tipos de operación:

(*a*) Imprimir un símbolo. (El imprimir un símbolo incluye el borrar primero el símbolo previo.) Borrar un símbolo, es decir, imprimir una *B*, en una operación de este tipo.
(*b*) Desplazarse un cuadro a la izquierda.
(*c*) Desplazarse un cuadro a la derecha.

Un *paso* operativo de la máquina es una operación aislada de uno de estos tipos.

Seguidamente hemos de especificar cómo escoge la máquina, en cada estadio del proceso, la operación a efectuar. Su curso de acción está determinado por el símbolo que aparece en el cuadro que se está leyendo y por el *estado interno* de la máquina. La máquina puede tomar cualquiera de entre un número finito de estados internos. En términos de las máquinas calculadoras reales, el estado interno puede concebirse

como la suma total de toda la información almacenada en la máquina en el instante dado. No vamos a ocuparnos de procedimientos mecánicos o electrónicos de almacenamiento de información — supondremos simplemente que nuestra caja negra tiene un número finito de condiciones diferentes que causan el que ella actúe de ciertos modos.

No obstante, está claro que hay que cuidarse de que el estado interno de la máquina de Turing cambie a lo largo de un cómputo, de modo que cada paso de un cómputo requerirá especificar:

(1) el estado interno actual de la máquina,
(2) el contenido del cuadro que se está leyendo,
(3) la acción efectuada por la máquina y
(4) el siguiente estado interno que la máquina toma en preparación del siguiente paso del cómputo.

Así pues, el estado interno que la máquina tiene en un instante dado será consecuencia del curso global del cómputo previo, y en este sentido los estados actúan como «memoria» de la máquina.

En este punto hemos de hacer de nuevo un comentario acerca de la condición de finitud impuesta al número de estados internos de una máquina de Turing. Los computadores digitales reales solamente tienen un número finito de configuraciones internas diferentes, si bien es verdad que este número es extremadamente grande. No obstante, por las mismas razones antes indicadas, no sería razonable el imponer ninguna cota específica, ni siquiera una muy grande, al número de estados permitidos para una máquina de Turing. Por lo tanto, nos limitaremos a exigir que sea un número finito.

El modo más conveniente de especificar el procedimiento seguido por una máquina de Turing es por medio de un conjunto finito de cuádruplas de la forma

(estado, símbolo de cinta, acción a efectuar, nuevo estado a tomar)

Para seguir la traza de un cómputo es preciso anotar en cada momento el estado interno y el símbolo de la cinta que se está leyendo, buscar en el conjunto de cuádruplas hasta encontrar una que comience por este par, ejecutar la acción indicada y tomar el nuevo estado dado por esta cuádrupla. Esto trae consigo una restricción que hay que imponer a nuestro conjunto de cuádruplas: Debe ser consistente, es decir, para cada par (estado, símbolo) debe haber a lo sumo una cuádrupla que empiece por ese par, de manera que la máquina de Turing tenga un procedimiento bien definido a seguir.

Como tanto el número de estados como el número de símbolos son finitos, hay un límite en el número de cuádruplas para una máquina particular. No obstante, no requeriremos que todo par de la forma

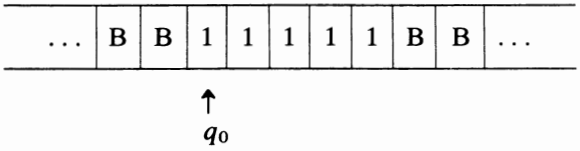
(estado, símbolo) aparezca al comienzo de alguna cuádrupla. Puede ser que algunas combinaciones no aparezcan nunca en un cómputo. Lo que es más importante, diremos que un cómputo de una máquina de Turing *termina* si y sólo si el par (estado, símbolo) actual no aparece en ninguna de las cuádruplas, de modo que la máquina carece de instrucción de cómo proceder.

Así pues, una máquina de Turing es capaz de transformar una cinta de entrada en una cinta de salida. El modo de simbolizar la información sobre la cinta depende forzosamente de la naturaleza de la información, y veremos mediante ejemplos cómo puede hacerse. En todos nuestros ejemplos usaremos símbolos q_0, q_1, q_2, ... para denotar estados internos, y convendremos en que las máquinas comienzan en estado q_0 leyendo el cuadro no blanco situado más a la izquierda en la cinta. (Algún convenio de este tipo es evidentemente necesario — éste que hemos tomado no tiene ninguna significación especial).

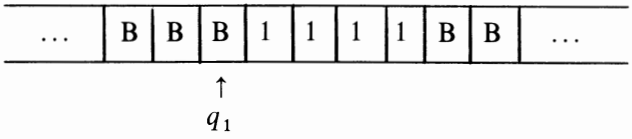
Ejemplo 7.12

$$[(q_0 \quad 1 \quad B \quad q_1), (q_1 \quad B \quad D \quad q_0)]$$

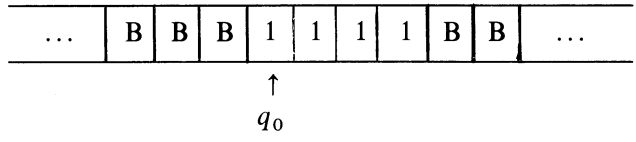
es el conjunto de cuádruplas de una máquina de Turing de estados q_0 y q_1, cuyo alfabeto de símbolos consta de B y 1. Las cuádruplas se explican a sí mismas, excepto quizás en lo referente a símbolos de «acción a efectuar». El tercer símbolo de una cuádrupla puede ser I («mover a la izquierda»), D («mover a la derecha») o simplemente el símbolo por el que hay que reemplazar el símbolo que se está leyendo. Obsérvese el modo de operación de esta máquina cuando la cinta de entrada contiene una sucesión finita de 1*s*, por ejemplo.



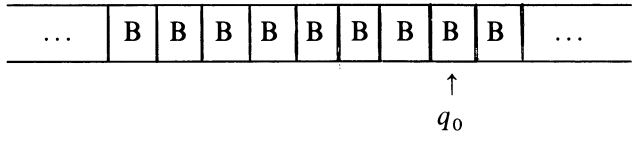
La máquina comienza en estado q_0 leyendo el 1 de más a la izquierda. Imprime un B (borra el 1) y pasa al estado q_1.



La máquina en estado q_1 y leyendo un B se mueve un cuadro a la derecha y pasa al estado q_0.



Ahora, lo mismo que arriba, el 1 del cuadro que se está leyendo se reemplaza por un B y la máquina pasa al estado q_1. Así pues, la máquina procederá a moverse a la derecha reemplazando cada 1 por un B, hasta que alcance la situación

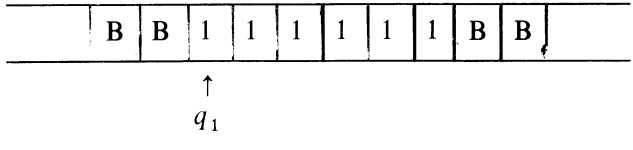


Ahora no existe ninguna cuádrupla capaz de guiar a la máquina en esta situación, de modo que el cómputo se detiene. Esta máquina borra una sucesión finita de 1s y se para.

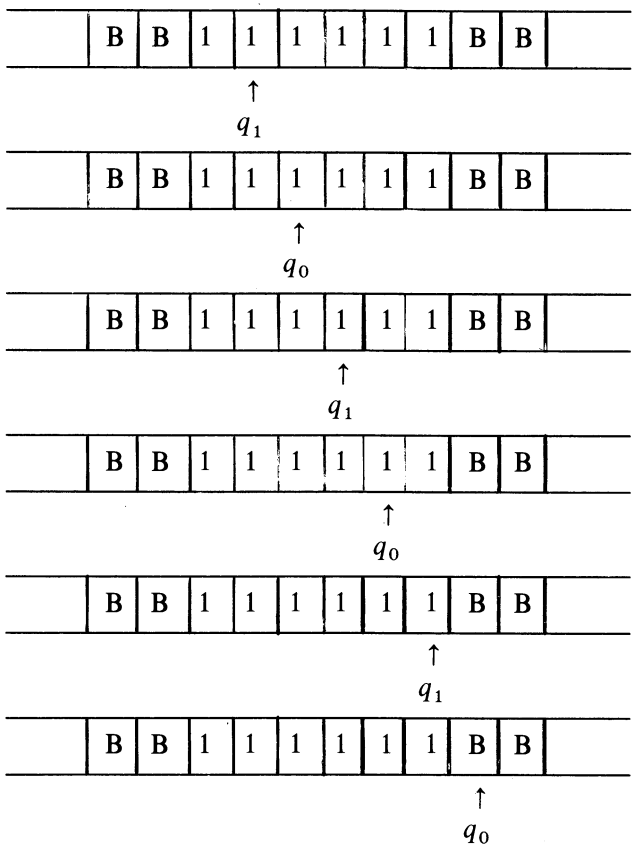
Ejemplo 7.13

$$\{(q_0\ 1\ D\ q_1), (q_1\ 1\ D\ q_0), (q_1\ \mathrm{B}\ D\ q_2), (q_2\ \mathrm{B}\ 1\ q_2)\}$$

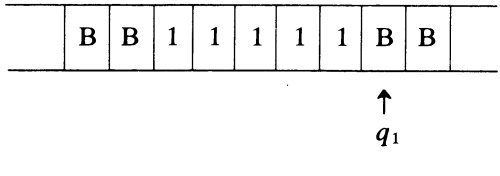
es el conjunto de cuádruplas de una máquina de Turing que decide si un número es par o impar del siguiente modo. Puede darse un número como entrada en forma de sucesión finita de 1s sobre la cinta. La máquina comienza en estado q_0 leyendo el 1 de más a la derecha. Por ejemplo,



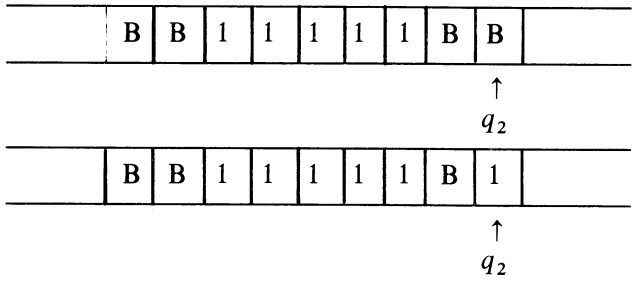
La máquina procede como sigue:



y para aquí, ya que no hay ninguna cuádrupla que comience por q_0B. Procederá análogamente para todo número par que se le dé como entrada. Si el número dado como entrada hubiese sido impar, habríamos alcanzado la situación (entrada 5)



y el cómputo proseguiría así:



deteniéndose aquí. Así pues, esta máquina imprimirá un 1 tras un espacio de un cuadro si y sólo si el número de entrada es impar.

Ejemplo 7.14

$$\{(q_0\ 1\ X\ q_0),\ (q_0\ X\ D\ q_0),\ (q_0\ 0\ Y\ q_0),\ (q_0\ Y\ D\ q_0)\}$$

es el conjunto de cuádruplas de una máquina de Turing que, dada una sucesión finita de 0s y 1s como entrada, la traducirá a una sucesión finita de Xs e Ys; p. ej., 1 0 1 0 0 1 se traduce como X Y X Y Y X. Pregunta: ¿Para esta máquina después de completar su traducción?

Ejemplo 7.15

La adición es casi trivial para una máquina de Turing. Si m y n se dan como entrada sobre la cinta en forma de sucesiones de 1s separadas por la letra A, la máquina cuyas cuádruplas son

$$\{(q_0\ 1\ B\ q_0),\ (q_0\ B\ D\ q_1),\ (q_1\ 1\ D\ q_1),\ (q_1\ A\ 1\ q_2)\}$$

borrará el 1 de más a la izquierda, reemplazará la A por un 1 y parará. Cuando para, el número $m+n$ ha quedado sobre la cinta en forma de sucesión de $(m+n)$ 1s.

Ejemplo 7.16

Una máquina de Turing puede reproducir el contenido de la cinta de entrada. Por ejemplo, si la cinta de entrada está en blanco exceptuando una sucesión finita de 0s y 1s, una tal máquina viene especificada por el conjunto de cuádruplas:

q_0 0 X q_1
q_1 X D q_1
q_1 0 D q_1
q_1 1 D q_1
q_1 B D q_3
q_3 0 D q_3
q_3 1 D q_3
q_3 B 0 q_5

q_0 1 Y q_2
q_2 Y D q_2
q_2 0 D q_2
q_2 1 D q_2
q_2 B D q_4
q_4 0 D q_4
q_4 1 D q_4
q_4 B 1 q_5

q_5 0 I q_5
q_5 1 I q_5
q_5 B I q_5

q_5 X D q_0

q_5 Y D q_0

q_0 B I q_6
q_6 X 0 q_6
q_6 Y 1 q_6
q_6 0 I q_6
q_6 1 I q_6

Este ejemplo es claramente más complicado que los anteriores, y las cuádruplas se han dispuesto de esta manera para hacer más claro el modo de proceder de la máquina. Sigamos su funcionamiento en un ejemplo sencillo. Supongamos que la cinta de entrada está en blanco exceptuando $\boxed{0\,1}$ y que la máquina comienza en estado q_0, leyendo el cuadro no blanco de más a la izquierda. Entonces la máquina empezará usando la columna de cuádruplas de la mano izquierda, y la cinta se procesará así:

B	0	1	B

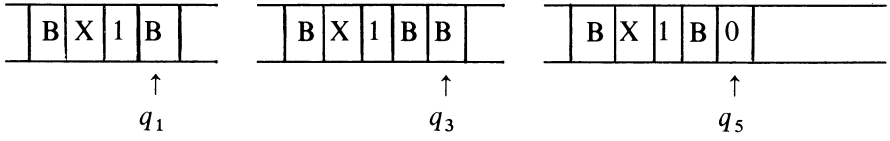
↑
q_0

B	X	1	B

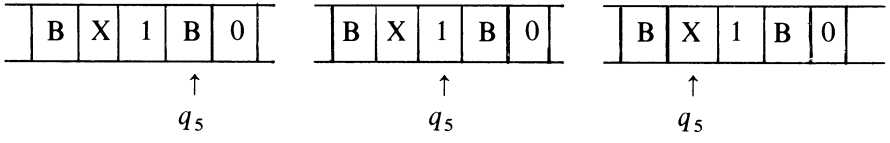
↑
q_1

B	X	1	B

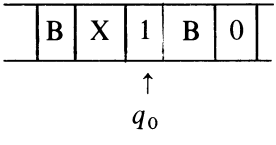
↑
q_1



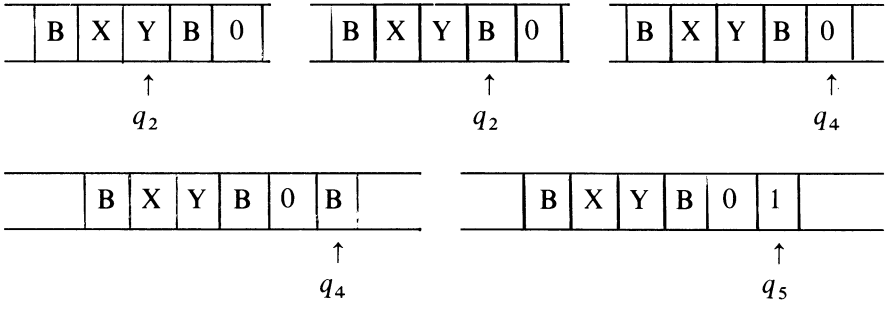
Seguidamente, la máquina usará la columna de cuádruplas central, dando



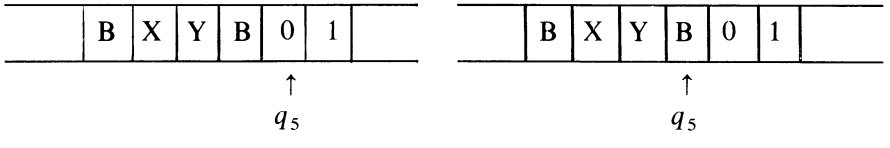
La cuádrupla q_5 X D q_0 da entonces

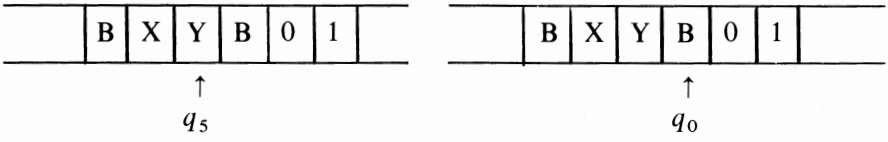


y pasamos a la cima de la columna de las cuádruplas de la mano derecha

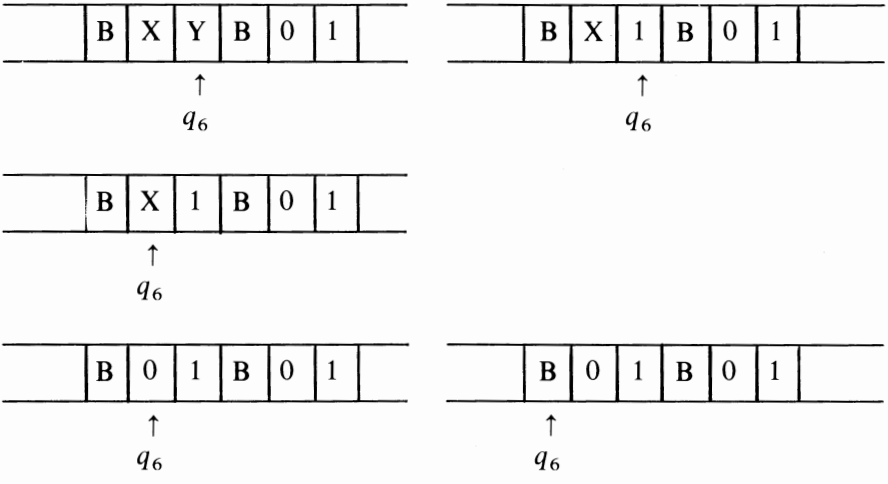


Es estado q_5, del mismo modo que antes, lleva a





Ahora, en estado q_0 y leyendo B se usan la columna de cuádruplas central inferior, resultando:



y aquí la máquina para, ya que no hay ninguna cuádrupla que empiece por q_0 B.

▷Este último ejemplo ilustra algunos de los procesos elementales de búsqueda, copia, memorización y repetición que una máquina de Turing puede usar para llevar a cabo procedimientos más complejos, e ilustrar asimismo cómo pueden encontrarse instrucciones (es decir, cuádruplas) para una máquina de Turing particular, analizando el procedimiento que se requiere seguir y descomponiéndolo en una sucesión de estos procesos elementales. Nótese que el tamaño del alfabeto de símbolos para la cinta tiene un efecto directo sobre el número de cuádruplas requerido. En particular, una máquina que hubiese de duplicar una cadena de 1s requeriría el mismo tipo de procedimiento que en el ejemplo anterior, pero necesitaría menos cuádruplas.

Ejemplo 7.17

En este ejemplo no entraremos en tantos detalles como en el anterior, pero se recomienda al lector que siga al menos un cómputo de la má-

quina con el fin de observar la combinación de procesos elementales involucrada y, en particular, el modo en que se utiliza el procedimiento de copia del ejemplo anterior. Las siguientes cuádruplas especifican una máquina de Turing que multiplica dos números m y n usando las dos entradas, en forma de sucesiones de m y n 1s, están separadas por un cuadro en blanco.

q_0 1 X q_1
q_1 X D q_1
q_1 1 D q_1
q_1 B D q_2
q_2 1 Y q_3
q_3 Y D q_3
q_3 1 D q_3
q_3 B D q_4
q_4 B 1 q_5
q_4 1 D q_4
q_5 q I q_5
q_5 B I q_5
q_5 Y 1 q_6
q_6 1 D q_2
q_2 B I q_7
q_7 1 I q_7
q_7 B I q_7
q_7 X B q_8
q_8 B D q_0
q_0 B D q_9
q_9 1 B q_{10}
q_{10} B D q_9

Esta máquina, partiendo por ejemplo de la cinta de entrada

...	B	1	1	B	1	1	1	B	...

comenzando en estado q_0 y leyendo el 1 de más a la izquierda, llegará a parar en estado q_9 con la cinta así:

	B	1	1	1	1	1	1	B	

↑
q_9

Esta máquina, pese a estar diseñada para un procedimiento más complicado que el ejemplo anterior, tiene menos cuádruplas. Ello se debe a que el alfabeto de símbolos para la cinta es más restringido.

Observación 7.18

En cualquier estadio de un cómputo de una máquina de Turing, solamente hay una parte finita de la cinta que no esté en blanco. Podemos, pues, representar la condición de la máquina mediante una «descripción instantánea», tal como por ejemplo

$$1\ 1\ \mathbf{B}\ 1\ \mathbf{B}\ q_2\ \mathbf{B}\ 1\ \mathbf{B}\ \mathbf{B}\ \mathbf{B}\ 1$$

Esto incluye toda la sección de cinta que no está en blanco y el cuadro que la máquina está leyendo. El símbolo del estado se incluye en la sucesión y se coloca inmediatamente a la izquierda del símbolo que se está leyendo. Es importante observar que no es necesario que una descripción instantánea contenga *solamente* la parte no blanca de la cinta. Por ejemplo,

$$q_5\ \mathbf{B}\ \mathbf{B}\ \mathbf{B}\ \mathbf{B}\ 1\ 1\ \mathbf{B}\ 1 \qquad \text{y} \qquad 1\ \mathbf{B}\ 1\ 1\ \mathbf{B}\ \mathbf{B}\ \mathbf{B}\ q_3\ \mathbf{B}$$

son descripciones instantáneas adecuadas al caso de que la máquina esté leyendo un cuadro en una parte blanca de la cinta. No obstante, nunca incluiremos más blancos de los necesarios para incluir el cuadro que se está leyendo.

Observación 7.19

Una máquina de Turing está especificada por su lista de cuádruplas. Mediante un sistema de codificación similar a la numeración de Gödel del Capítulo 6, es posible asignar números de código primero a las propias cuádruplas y luego a las listas finitas de cuádruplas. Esto es debido a que (podemos suponer que) todos los posibles símbolos de estado y símbolos para la cinta constituyen un conjunto numerable, y cada máquina de Turing usa sólo un número finito de ellos. Por lo tanto, podemos asignar a cualquier máquina de Turing un número de código, y si el método de descripción (tomando en consideración el estado inicial y el modo en que se codifican las entradas y las salidas) se estandariza, los números de código serán tales que toda la información relevante acerca de las correspondientes máquinas de Turing será efectivamente recuperable. Exactamente igual que antes, escogemos los números de código de modo que diferentes números de código correspondan a diferentes máquinas. También será posible decidir efectivamente si un número natural arbitrario dado es el número de código de una máquina de Turing. No vamos a demostrar esto porque depende de los detalles del sistema de código elegido, pero ello lleva a un importante resultado.

Proposición 7.20

La colección de (los números de código de) las máquinas de Turing es efectivamente enumerable.

Demostración: Enumérense todos los números naturales y, a medida que vayan apareciendo, bórrense todos los números que no sean números de código de máquinas de Turing.

▷ Esta enumeración efectiva nos permite asociar de modo efectivo la lista de las máquinas de Turing con el conjunto de todos los números naturales. Cada máquina de Turing corresponderá al número dado por su posición en la lista. Podemos, pues, tomar el conjunto de números de código de máquina de Turing como el conjunto de todos los números naturales. Tenemos la siguiente proposición.

Proposición 7.21 (El Teorema de Enumeración)

El conjunto de todas las máquinas de Turing puede enumerarse en una lista T_0, T_1, T_2, ... de tal modo que cada subíndice determine de manera efectiva y completa las instrucciones de la máquina correspondiente.

▷ Nuestros ejemplos de máquinas de Turing han mostrado que éstas son capaces de efectuar varias clases de cómputos. Estamos interesados en un tipo particular de cómputo, a saber, el cómputo de los valores de una función. Ahora bien, de *cualquier* máquina de Turing puede decirse que calcula los valores de una función, con tal que especifiquemos el modo de interpretar los contenidos de las cintas de entrada y salida como elementos del dominio y del rango de la función. Nuestras funciones van a ser aritméticas, es decir, sus dominios y rangos van a constar de números naturales. Un elemento n de D_N puede darse como entrada a cualquier máquina de Turing como sucesión de n 1s sobre la cinta blanca en el resto de los cuadros. Si subsiguientemente la máquina para, el número de salida puede tomarse como el número de cuadros de la cinta que en ese momento no están en blanco. No hay ninguna razón para escoger esta representación en lugar de otras, pero es importante ser específico en este punto, porque requerimos que a cada máquina de Turing vaya asociada una única función (parcial). Nótese que estos convenios dan lugar a funciones de una variable. Si considerásemos los cómputos de máquinas de Turing cuando sus cintas de entrada tienen un par de números representados sobre ellos (por ejemplo, de la manera descrita en el Ejemplo 7.15), entonces las máquinas se asociarían a funciones de dos variables. Está claro que podemos tratar un número mayor de variables de manera similar.

Observación 7.22

(*a*) Se sabe que para toda función aritmética que sea calculable mediante una máquina de Turing, existe una máquina de Turing que computa los valores de f y cuyo alfabeto de símbolos para la cinta es

{B, 1}. No vamos a demostrar esto, pero es consecuencia del hecho de que el alfabeto de cualquier máquina de Turing es finito, y sus símbolos pueden codificarse como números en notación binaria, usando el símbolo B en lugar de 0.

(*b*) Se sabe también que para toda función aritmética que sea calculable mediante una máquina de Turing, existe una máquina de Turing que computa f y que tiene solamente dos estados internos. Tampoco demostraremos esto, pero haremos notar que esta reducción del número de estados solamente es posible ampliando considerablemente el alfabeto de símbolos para la cinta. Puede reducirse a dos el número de estados o el número de símbolos, pero, en general, no ambos a un tiempo. (Véase Minsky, Capítulo 6.)

Definición 7.23

Una función (parcial) aritmética es *Turing-computable* si existe una máquina de Turing que computa sus valores, bajo los convenios especificados más arriba acerca de la entrada y la salida.

Hasta ahora no tenemos ninguna información referente a la posibilidad de que una sola función corresponda de este modo a más de una máquina de Turing, pero ahora podemos precisar.

Proposición 7.24

Para cada función (parcial) Turing-computable f existen infinitas máquinas de Turing que computan los valores de f.

Demostración: Dadas f y una máquina de Turing T que calcule sus valores, supongamos que $q_0, \ldots, q_k$ sean los estados internos de T. Añadamos la cuádrupla q_{k+1} 1 1 q_{k+1}, obteniendo una nueva máquina de Turing T^1. T^1 computa los valores de f, ya que la nueva cuádrupla no tiene efecto sobre ninguno de los cómputos (el estado q_{k+1} no se toma nunca). Análogamente, podemos generar una sucesión T^2, T^3, ... de máquinas de Turing, añadiendo sucesivamente las cuádruplas q_{k+2} 1 1 q_{k+2}, q_{k+3} 1 1 q_{k+3}, ... Cada una de estas máquinas computa los valores de f.

Observación: Es importante notar la distinción que aparece aquí entre una función y un conjunto de instrucciones para calcular sus valores. Las máquinas de Turing a las que nos hemos referido en la demostración anterior son diferentes, puesto que tienen diferentes conjuntos de cuádruplas, pero las diferencias son inesenciales en tanto que no afectan a los cómputos a efectuar.

▷Turing postuló (en 1936) que había tenido éxito en hacer lo que se

había propuesto, es decir, caracterizar de un modo matemáticamente preciso, por medio de sus máquinas, la clase de las funciones computables mediante un algoritmo; y el enunciado siguiente se conoce hoy como la *Tesis de Turing:*

> La clase de las funciones (parciales) Turing-computables coincide con la clase de las funciones (parciales) computables mediante un algoritmo.

Un modo equivalente de enunciar esto es decir que todo algoritmo (o conjunto de instrucciones) para computar los valores de una función parcial f puede traducirse (efectivamente) a un conjunto de cuádruplas que defina una máquina de Turing que compute los valores de f.

Como ya se observó anteriormente, no podemos esperar demostrar la Tesis de Turing, porque ésta involucra una noción intuitiva (la de algoritmo). No obstante, una gran cantidad de trabajo de investigación ha llevado a muchos resultados que apoyan la Tesis de Turing. Uno de ellos es el siguiente:

Proposición 7.25

Una función (parcial) aritmética es Turing-computable si y sólo si es una función (parcial) recursiva.

Demostración: La demostración de esto es muy técnica, ya que involucra necesariamente todo el detalle de las definiciones de máquina de Turing y de función recursiva. Es demasiado extensa para incluirla aquí, pero remitimos al lector interesado al libro de Minsky.

▷ Naturalmente, a la luz de esto la Tesis de Turing resulta ser equivalente a la de Church.

Proposición 7.26

Existe una enumeración efectiva $\varphi_0, \varphi_1, \varphi_2, \ldots$ de las funciones parciales recursivas de una variable, en la cual cada función parcial recursiva aparece infinitas veces.

Demostración: Esto es una consecuencia inmediata de las Proposiciones 7.21, 7.24 y 7.25.

▷ Hasta aquí la descripción de las máquinas de Turing y de lo que hacen. Llevemos ahora las cosas un paso más hacia adelante y descubramos a qué nos conducen en relación con problemas de decisión y solubilidad.

Consideremos el siguiente algoritmo: Dado cualquier par de números $m, n \in D_N$, enumérese la lista $T_0, T_1, T_2, \ldots$ de máquinas de Turing

hasta alcanzar T_m y sígase el cómputo de T_m aplicado a la entrada n. Este es un algoritmo para calcular los valores de una función (parcial) de dos variables. Por la Tesis de Turing existe entonces una máquina de Turing que calcula los valores de esta función. Podemos enunciar esto en forma de proposición.

Proposición 7.27

Existe una *máquina de Turing universal.* Es decir, existe una máquina de Turing T que, cuando se interpreta como máquina que calcula los valores de una función de dos variables m y n, lleva a cabo el cómputo de la máquina T_m con entrada n.

▷ La máquina universal puede, pues, ejecutar el procedimiento de cualquiera de las máquinas $T_0, T_1, T_2, \ldots$ en el cálculo de funciones de una variable. Esto es una indicación tanto de la potencia como de las limitaciones de las máquinas de Turing. La máquina universal es aparentemente un objeto complejo y potente, ya que comprende las capacidades de todas las máquinas de una variable. Pero, por otra parte, las complejidades de $T_0, T_1, \ldots$ están limitadas por la complejidad de la máquina universal.

Consideremos el siguiente algoritmo: Dado $n \in D_N$ arbitrario, encuéntrese φ_n en la lista de las funciones parciales recursivas, y sígase el cómputo (usando T_n) de $\varphi_n(n)$. En caso de que se obtenga un resultado, súmesele 1. Por la Tesis de Church, este algoritmo define una función parcial recursiva; sea ésta φ_{k_0}. Preguntémonos ahora: ¿Cuál es el resultado del cálculo del valor de $\varphi_{k_0}(k_0)$? Siguiendo el algoritmo, obtenemos la contradicción

$$\varphi_{k_0}(k_0) = \varphi_{k_0}(k_0) + 1.$$

No obstante, para llegar aquí hemos pasado por alto un punto: El cálculo de $\varphi_{k_0}(k_0)$ puede no terminar. De hecho, de lo anterior podemos deducir que no termina, pues en otro caso no hay modo de salir de la contradicción.

Lo anterior muestra el modo en que podemos usar las enumeraciones $T_0, T_1, \ldots$ y $\varphi_0, \varphi_1, \ldots$ para describir algoritmos. Este procedimiento lleva a problemas interesantes. También puede usarse del modo siguiente:

Proposición 7.28

No existe ninguna enumeración efectiva $f_0, f_1, \ldots$ de todas las funciones (totales) recursivas de una variable.

Demostración: Supongamos lo contrario, es decir, sea $f_0, f_1, f_2, \ldots$ una enumeración efectiva de todas las funciones totales recursivas de una

variable (eventualmente con repeticiones). Consideremos el siguiente algoritmo: Dado $n \in D_N$, enumérense $f_0, f_1, \ldots$ hasta obtener f_n. Compútese $f_n(n)$ y súmese 1. Por la Tesis de Church, esta función h, que verifica

$$h(n) = f_n(n) + 1 \text{ para cada } n \in D_N,$$

es recursiva, y es total, puesto que cada f_n es total. Por lo tanto, $h = f_k$ para algún k. Así pues:

$$h(k) = f_k(k) = f_k(k) + 1$$

Esta vez no hay escape de la contradicción, y queda demostrado nuestro resultado.

>Sería conveniente si pudiera decirse de antemano si un cómputo de máquina de Turing dado va a terminar. Por ello, el problema de decidir, para un par dado m, $n \in D_N$, si la máquina de Turing T_m parará con entrada n, es problema que ha sido investigado. Se le llama *Problema de Parada* para máquina de Turing. Su importancia se debe en no poca medida al siguiente resultado.

Proposición 7.29

El Problema de Parada para máquinas de Turing es insoluble, es decir, no existe ningún algoritmo que dé respuesta a preguntas del conjunto

$$\{\text{¿Para la máquina } T_m \text{ con entrada } n?/m,\ n \in D_N\}.$$

Demostración: Por la Tesis de Turing será suficiente que demostremos que la función f: $D_N \to D_N$ dada por

$$f(n) = \begin{cases} 0 & \text{si } T_n \text{ se para sobre la entrada } n \\ 1 & \text{si } T_n \text{ no se para sobre la entrada } n \end{cases}$$

no es Turing computable. En efecto, supongamos que existiese un algoritmo para responder a preguntas del conjunto de más arriba. Entonces existiría un algoritmo para responder a preguntas del conjunto:

$$\{\text{¿Para la máquina } T_n \text{ con entrada } n?/n \in D_N\},$$

y, por tanto, existiría un algoritmo para calcular los valores de la función f de más arriba. Esto no puede ocurrir si f no es Turing computable.

Concentrémonos, pues, en f, y supongamos que es Turing computable y que la máquina de Turing T computa sus valores. Entonces, para

entrada n, T parará dando salida 0 ó 1 según que T_n pare o no con entrada n. Modifiquemos T para obtener una máquina de Turing T' tal que para todo n,

$$* \begin{cases} \text{si} & T_n \text{ para con entrada } n, \ T' \text{ no para con entrada } n, \text{ y} \\ \text{si} & T_n \text{ no para con entrada } n, \ T' \text{ para con entrada } n. \end{cases}$$

T' se obtiene a partir de T incluyendo nuevos estados y cuádruplas que tienen el efecto de añadir a todo cálculo de T que pare, una búsqueda de un cuadro no blanco sobre la cinta de salida. Si la búsqueda tiene éxito, T' para, y en otro caso T' continúa buscando indefinidamente. La búsqueda puede tener éxito (habiendo partido T' con entrada n) si y sólo si hay un 1 sobre la cinta en este último estadio, es decir, si y sólo si T_n no para con entrada n. (Para dar detalles: Podríamos incluir dos nuevos estados, q_α y q_β, y las siguientes cuádruplas: $q_i \ S \ R \ q_\alpha$, para todo $q_i \ S$ que no aparezca como primer par en una cúadrupla de T (siendo S un símbolo de cinta) y q_α B A q_β, q_α A D q_α, q_β A I q_β, q_β B A q_α.)

La máquina T' deberá aparecer en la lista $T_0, T_1, T_2, \ldots$ Supongamos que T' es T_{n_0}. Planteemos ahora la pregunta crucial: ¿Para T_{n_0} con entrada n_0? Volvamos a * de más arriba. Lo que allí se dice es: T_{n_0} para con entrada n_0 si y sólo si T_{n_0} no para con entrada n_0. Esta clara contradicción basta para indicarnos que f no puede ser Turing computable, y el resultado de la proposición queda demostrado.

▷ Consideremos ahora el siguiente algoritmo: Dado cualquier $n \in D_N$, búsquese en la lista $T_0, T_1, T_2, \ldots$ hasta alcanzar T_n, y sígase entonces el cálculo de la máquina T_n con entrada n. En caso de que el cálculo pare, dése salida 1. Por la Tesis de Turing, la función cuyos valores son calculados por este algoritmo es Turing computable. Esta función, llamémosla φ, viene dada por

$$\varphi(n) = \begin{cases} 1 \text{ si } T_n \text{ para con entrada } n, \\ \text{indefinida en otro caso} \end{cases}$$

Está claro que φ es una función parcial, ya que ciertamente hay máquinas de Turing que no paran para ninguna entrada y otras que paran solamente para algunas entradas. El dominio de φ es un conjunto importante en este campo de estudio y se denota generalmente por K.

$$K = \{n \in D_N : T_n \text{ para con entrada } n\}.$$

Ahora bien, es consecuencia de la demostración de la Proposición 7.29 que K no es un conjunto recursivo (bajo la hipótesis de la Tesis de Church, por supuesto), ya que si lo fuese existiría un algoritmo para

responder a preguntas de la forma «¿$n \in K$?» para $n \in D_N$, es decir, preguntas del conjunto

$$\{\text{¿Para la máquina } T_n \text{ con entrada } n?/n \in D_N\}.$$

Proposición 7.30

K es un conjunto recursivamente enumerable y no recursivo.

Demostración: K no es recursivo, por lo visto más arriba. Que K es recursivamente enumerable puede demostrarse dando un algoritmo que lo enumera.

Paso 1. Sígase un paso del cómputo de T_0 con entrada 0.
Paso 2. Sígase un paso del cómputo de T_1 con entrada 1 y el segundo paso del cómputo de T_0 con entrada 0.
Paso 3. Sígase un paso del cómputo de T_2 con entrada 2, el segundo paso del cómputo de T_1 con entrada 1 y el tercer paso del cómputo de T_0 con entrada 0.

etcétera. Cuando una de las máquinas T_i pare, póngase i en la enumeración de K e ignórense todas las referencias a T_i en los pasos subsiguientes del algoritmo. Para cada $n \in K$ se llegará a un paso en el que T_n con entrada n para, y n se pondrá en la enumeración de K. K es, pues, efectivamente enumerable, y por tanto, según la Tesis de Church, recursivamente enumerable.

Proposición 7.31

Para toda máquina de Turing T, el dominio de T, es decir, el conjunto de todos los $n \in D_N$ para los que T para con entrada n, es un conjunto recursivamente enumerable (que, por supuesto, puede ser recursivo).

Demostración: La demostración es muy similar a la anterior, siguiendo los cómputos, esta vez de la misma máquina T, para diferentes entradas, haciendo simultáneamente una lista de todos los números de entrada para los que T para.

$\triangleright K$ es un ejemplo concreto de conjunto no recursivo, surgido de la consideración de máquinas de Turing y el Teorema de Enumeración. Existen muchos otros. Por ejemplo:

Ejemplo 7.32

(*a*) $\{n \in D_N$: T_n para con cualquier entrada$\}$ no es recursivo, ni recursivamente enumerable.
(*b*) $\{n \in D_N$: T_n no para con ningún input$\}$ no es ni recursivo, ni recursivamente enumerable.

(*c*) Para cada n_0 fijo, el conjunto $\{n \in D_N : T_n$ para con entrada $n_0\}$ no es recursivo, pero es recursivamente enumerable.

Estos ejemplos nos dan también clases de cuestiones recursivamente insolubles, de acuerdo con la Definición 7.11.

(*d*) $\{$¿Se tiene $n \in K? / n \in D_N\}$

(*e*) $\{$¿Para T_n con toda entrada$? / n \in D_N\}$

(*f*) $\{$¿Para T_n con alguna entrada$? / n \in D_N\}$

(*g*) $\{$¿Para T_n con entrada $n_0? / n \in D_N\}$, siendo n_0 cualquier número fijo.

Estas clases de problemas son recursivamente insolubles.

El método usado para verificar todos estos resultados es similar. Consiste en suponer que el conjunto es recursivo (o que la clase de problemas es recursivamente soluble) y deducir de ello que el conjunto K es recursivo (o que cualquier otro conjunto del que se sabe que no es recursivo, es recursivo). Este método puede considerarse desde dos puntos de vista. En primer lugar, puede considerarse simplemente como una demostración por contradicción. En segundo lugar, puede verse dentro de un contexto más amplio como introductor de una nueva idea, la de *reducibilidad.*

Definición 7.33

El conjunto A es *reducible* al conjunto B si es cierto que la existencia de un algoritmo para decidir la pertenencia a B garantizaría la existencia de un algoritmo para decidir la pertenencia al conjunto A.

Puede ser que ninguno de los dos algoritmos exista, pero a menudo resulta interesante descubrir si dos conjuntos están relacionados de esta manera. Un ejemplo obvio de una tal reducibilidad es el resultado de que $D_N \backslash K$ es reducible a K, pese a que no existe algoritmo para decidir la pertenencia a ninguno de los dos conjuntos. No obstante, aquí no vamos a ocuparnos de este tipo de ideas, y remitimos al lector interesado al libro de Rogers para mayor información.

▷Esto concluye nuestra investigación de las máquinas de Turing. Ahora procederemos a usar las ideas y técnicas que hemos desarrollado en una discusión de resultados de insolubilidad e indecidibilidad.

Ejercicios

7 Modifíquese la máquina de Turing del ejemplo 7.12 de modo que borre todos los símbolos que aparezcan sobre la cinta de entrada. (Según está, la máquina borrará 1*s* hasta llegar a un *B*, en el que parará, de modo que si la cinta de entrada tiene un cierto número de 1*s* salteados, no todos serán borrados.)

8 Modifíquese la máquina de Turing del ejemplo 7.13 de manera que pare dejando la

cinta completamente en blanco si el número de entrada es par, y pare dejando un solo 1 en la cinta si el número de entrada es impar.

9 Constrúyase una máquina de Turing cuyo alfabeto de símbolos para la cinta sea $\{B, 1\}$ y que no pare para ninguna cinta de entrada.

10 Constrúyase una máquina de Turing tal que cuando la cinta de entrada contenga una sola sucesión finita de 1*s* pare dejando sobre la cinta dos sucesiones finitas de 1*s* de esa misma longitud, separadas por el símbolo X.

11 Constrúyase una máquina de Turing T que calcule los valores de la función parcial f definida por:

$$f(n) = \begin{cases} n \text{ si } n \text{ es impar} \\ \text{indefinida si } n \text{ es par} \end{cases}$$

Modifíquese T para obtener una máquina de Turing T' que se comporte como T si el número de entrada es impar, pero que pare dejando la cinta en blanco si el número de entrada es par. Dese un ejemplo de una función parcial Turing calculable para la que no sea posible llevar a cabo el proceso anterior.

12 Sea T una máquina de Turing cuyo conjunto de cuádruplas no contenga ninguna instrucción para mover a la izquierda. Diséñese un procedimiento efectivo para decidir de antemano, para cualquier cinta de entrada, si T llegará a parar.

13 A las máquinas de Turing cuyas instrucciones solamente permiten mover en un sentido a lo largo de la cinta se les llama a veces autómatas finitos. Demuéstrese que el problema de parada para autómatas finitos es resoluble.

14 Demuéstrese que $\bar{K}$ no es recursivamente enumerable.

15 Sea A un subconjunto recursivamente enumerable de $\bar{K}$ y supongamos que para alguna máquina de Turing T_n, $A = \{x : T_n \text{ para a partir de la entrada } x\}$. Demuéstrese que $n \in \bar{K} \setminus A$.

16 Demuéstrese que todo conjunto recursivamente enumerable es el dominio de alguna máquina de Turing.

17 Demuéstrese que las clases de problemas del ejemplo 7.32 son todas recursivamente insolubles.

18 Sea $K_0 = \{(m, n)$: La máquina de Turing T_m para a partir de la entrada $n\}$. Demuéstrese que K es reducible a K_0 y que K_0 es reducible a K.

7.3. Problemas de palabras

Un área en la que el álgebra y la lógica se interrelacionan es aquélla en la que se consideran problemas de palabras para sistemas algebraicos tales como grupos, semigrupos y grupos abelianos. El caso de los semigrupos es el más sencillo de describir, por lo que lo usaremos como ilustración.

Sea $A = \{a_1, \ldots, a_k\}$ un conjunto de símbolos formales. Este conjunto se considerará como un alfabeto, y las *palabras* sobre este alfabeto son precisamente las cadenas finitas de símbolos del alfabeto (no se impone ninguna restricción acerca de qué cadenas son palabras). Denotemos por S_A al conjunto de todas las palabras sobre el alfabeto A. S_A puede considerarse entonces como un semigrupo bajo la operación

de yuxtaposición. Para cada dos palabras de S_A puede formarse una palabra combinación, colocando la segunda tras la primera. Esta operación es automáticamente asociativa, de manera que S_A es un semigrupo. Si convenimos que la palabra vacía (una palabra que no contiene ningún símbolo) pertence a S_A, entonces dicha palabra actúa como identidad del semigrupo.

Un problema de palabras surge cuando un semigrupo tal como el S_A considerado arriba se modifica requiriendo que satisfaga una o más relaciones. Podemos ilustrar esto por medio de un ejemplo.

Ejemplo 7.34

Consideremos S_A como más arriba, y estipulemos que las palabras a_1a_2 y a_2a_1 se han de identificar entre sí. A partir de aquí, definimos una relación de equivalencia sobre S_A como sigue: Si P y Q son palabras, entonces $P\,a_1\,a_2\,Q \sim P\,a_2\,a_1\,Q$ y $P\,a_2\,a_1\,Q \sim P\,a_1\,a_2\,Q$, y para palabras cualesquiera U y V, U es *equivalente* a V si hay una sucesión de palabras $W_1, \ldots, W_n$ tal que $U = W_1$, $W_1 \sim W_2, \ldots, W_{n-1} \sim W_n$ y $W_n = V$. Es fácil demostrar que esto es una relación de equivalencia y que la operación de semigrupo está bien definida sobre las clases de equivalencia. (El lector observará que $\sim$ no es una relación de equivalencia - no es transitiva). El conjunto S_A^* de clases de equivalencia forma semigrupo. Es el semigrupo con generadores $a_1, \ldots, a_k$ y *relación* $a_1a_2 = a_2a_1$. El problema de palabras para S_A^* es decidir, para dos palabras dadas cualesquiera U y V, si son equivalentes, es decir, si representan el mismo elemento de S_A^*.

▷ Mas en general, podemos considerar semigrupos obtenidos a partir de S_A incluyendo un cierto número de relaciones de la forma $P_1 = Q_1$, $P_2 = Q_2, \ldots, P_m = Q_m$, siendo $P_1, \ldots, P_m, Q_1, \ldots, Q_m$ palabras dadas del alfabeto A. En este caso definimos $\sim$ poniendo

$$P\,P_i\,Q \sim P\,Q_i\,Q$$

para palabras cualesquiera P, Q y $1 \leqslant i \leqslant m$, y definimos la relación de equivalencia igual que antes. El conjunto de las clases de equivalencia se llama semigrupo de generadores $a_1, \ldots, a_k$ y relaciones $P_i = Q_i$ $(1 \leqslant i \leqslant m)$. El problema de palabras para este semigrupo es el análogo al anterior, pero evidentemente será más complicado cuantas más relaciones haya.

Definición 7.35

Un semigrupo está *finitamente presentado* si se ha obtenido como más arriba a partir de un conjunto finito de generadores y un conjunto finito de relaciones.

El problema de palabras para un semigrupo finitamente presentado es *recursivamente soluble* si existe un algoritmo que decide, dado cualquier par de palabras, si éstas son equivalentes.

El «Problema de Palabras para semigrupos» es: ¿existe un algoritmo que decida, dado cualquier semigrupo finitamente presentado y un par de palabras cualesquiera de él, si éstas son equivalentes?

Ejemplo 7.36

Sea $A=\{a_1, a_2\}$ y consideremos el semigrupo S generado por A sujeto a la relación $a_1\, a_2 = a_2\, a_1$. Podemos ver que el problema de palabras de este semigrupo es recursivamente soluble, describiendo un algoritmo del modo siguiente:

Toda palabra que involucre justamente a_1 y a_2 puede reordenarse paso a paso, usando cada vez la relación $a_1 a_2 = a_2 a_1$, hasta obtener una palabra en la que cada intervención de a_1 precede a cada intervención de a_2. Esta palabra es equivalente a la palabra original. (Por ejemplo, $a_2\, a_1\, a_2\, a_2 \sim a_2\, a_1\, a_1\, a_2 \sim a_1\, a_2\, a_1\, a_2 \sim a_1\, a_1\, a_2\, a_2$). Para el problema de palabras, dadas dos palabras cualesquiera P y Q, efectúese este procedimiento para cada una. P y Q son equivalentes si y sólo si las palabras resultantes son idénticas.

▷Como hemos observado previamente, si existe un algoritmo para una cierta clase de cuestiones, el encontrarlo y describirlo suele ser posible sin métodos ni hipótesis especiales. Por otra parte, para demostrar que no existe ningún algoritmo, prácticamente el único método que tenemos abierto es a través de la Tesis de Church. De hecho, existen semigrupos finitamente presentados cuyo problema de palabras no es recursivamente soluble. La demostración que vamos a dar de esto descansa enteramente sobre las ideas y métodos que hemos desarrollado en relación con máquinas de Turing, así que veamos primero estas dos nociones: La de máquina de Turing y la de semigrupo finitamente presentado.

Hemos visto cómo la condición en que se encuentran una máquina de Turing y su cinta en un momento dado puede especificarse mediante una descripción instantánea, consistente en una cadena de símbolos, por ejemplo

$$1\ \mathbf{B}\ 1\ 1\ \mathbf{B}\ q_i\ 1\ \mathbf{B}\ 1,\ 1\ 1\ 1\ 1\ \mathbf{B}\ 1\ \mathbf{B}\ q_i\ \mathbf{B}$$

Lo que haremos es considerar estas cadenas de símbolos como palabras, y considerar dos palabras como equivalentes si una de ellas se transforma en la otra mediante una sucesión finita de operaciones de la máquina de Turing. Veremos que hay ciertas complicaciones, pero a partir de nuestra máquina de Turing tomaremos nuestro alfabeto A de modo que incluya todos los símbolos para la cinta y para los estados,

y tomaremos las relaciones del semigrupo como las dadas por las cuádruplas de la máquina de Turing. Por ejemplo, si q_1 1 B q_2 es una de las cuádruplas, diremos que

$$P\ q_1\ 1\ Q \sim P\ q_2\ B\ Q$$

siendo P y Q cadenas cualesquiera de símbolos de A. Naturalmente, solamente algunas cadenas de símbolos de A tendrán de hecho la forma de una descripción instantánea de la máquina de Turing —algunas cadenas contendrán, por ejemplo, más de un símbolo de estado—. Nos encontraremos con que esto no tiene importancia. Pero ahora, especifiquemos:

Sea T la máquina de Turing que para si y sólo si la entrada α pertenece al conjunto K (K es recursivamente enumerable, pero no recursivo). Supondremos que T tiene como únicos símbolos de cinta 1 y B, y que el número α se da como entrada en forma de sucesión de α 1s. Denotemos a los estados internos de T por $q_0, \ldots, q_n$, y sea I el conjunto de cuádruplas de T. Tomemos

$$A = \{q_0,\ q_1,\ \ldots,\ q_n,\ q,\ q',\ 1,\ B,\ h\}$$

y consideremos el conjunto S_A de las palabras sobre este alfabeto. (La razón de que se incluyan los símbolos q, q' y h se explicará más abajo.) Denótese por $\mathcal{S}$ al semigrupo finitamente presentado con alfabeto A y con las relaciones siguientes. (Las letras X e Y se usan para denotar símbolos de cinta arbitrarios, 1 o B, a lo largo de lo que sigue.)

1. $q_i\ X = q_j\ Y$ si q_i X Y $q_j \in I$.
2. $q_i\ X\ Y = X\ q_j\ Y$ si $q_i\ X\ D\ q_j \in I$
   $q_i\ X\ h = X\ q_j\ B\ h$
3. $X\ q_i\ Y = q_j\ X\ Y$ si $q_i\ Y\ I\ q_j \in I$
   $h\ q_i\ Y = h\ q_j\ B\ Y$
4. $q_i\ X = q\ X$ si no hay ninguna cuádrupla de I que empiece por $q_i\ X$.
5. $q\ X = q$
6. $X\ q' = q'$.
7. $q\ h = q'\ h$.

Hemos incluido relaciones no sólo en correspondencia con las instrucciones de la máquina de Turing, sino también para gobernar el comportamiento de q, q' y h. Las descripciones instantáneas de la máquina se han de corresponder con palabras de S_A limitadas por h en ambos extremos. La condición inicial de la máquina podría ser q_0 1 1 1 1. La consideraremos representada por la palabra $h\ q_0$ 1 1 1 1 h. Las hs delimitan la parte significativa de la cinta. La máquina transforma su cinta de entrada paso a paso, y en pasos paralelos a éstos nuestra palabra es transformada en palabras equivalentes mediante aplicacio-

nes de relaciones. Las relaciones en 2 y 3 que involucran h nos permiten extender la palabra insertando un B en un extremo cuando sea necesario (es decir, cuando la máquina lea un cuadro que esté fuera de la parte no blanca de la cinta). Nótese lo que pasa cuando la máquina para. La máquina ya no modifica su cinta, pero podemos seguir transformando nuestra palabra usando las relaciones 4-7. Examinemos un ejemplo para ver lo que ocurre. Supongamos que la máquina ha parado y que nuestra palabra era en ese momento

$$h\ 1\ \mathbf{B}\ \mathbf{B}\ q_i\ 1\ 1\ h.$$

Ninguna cuádrupla de I empieza entonces por q_i 1; la relación 4 se aplica y

$$h\ 1\ \mathbf{B}\ \mathbf{B}\ q\ 1\ 1\ h,$$

es una palabra equivalente. La relación 5 lleva a las palabras equivalentes

$$h\ 1\ \mathbf{B}\ \mathbf{B}\ q\ 1\ h,$$

y

$$h\ 1\ \mathbf{B}\ \mathbf{B}\ q\ h.$$

La relación arroja entonces

$$h\ 1\ \mathbf{B}\ \mathbf{B}\ q'\ h,$$

y la relación de las palabras equivalentes

$$h\ 1\ \mathbf{B}\ q'\ h,$$

$$h\ 1\ q'\ h,$$

$$h\ q'\ h.$$

Esta palabra final no depende del contenido final de la cinta. De hecho, lo que podemos decir es que la máquina T con entrada α para si y sólo si la palabra $h\ q_0\ \alpha\ H$ es equivalente a $h\ q'\ h$. Esto es lo que nos permite demostrar que $\mathscr{S}$ es un semigrupo con problema de palabras recursivamente insoluble.

Proposición 7.37

Existe un semigrupo finitamente presentado cuyo problema de palabras es recursivamente insoluble.

Demostración: Sea $\mathscr{S}$ como se ha descrito más arriba. Supongamos que existe un algoritmo para decidir, para cualquier par de palabras de $\mathscr{S}$, si son equivalentes. Entonces existe un algoritmo para decidir la pertenencia al conjunto E, siendo

$$E = \{W \in S_A : W \text{ es equivalente a } h\ q'\ h\}$$

Ahora bien, T para con entrada α si y sólo si $\alpha \in K$. Así pues, para decidir la pertenencia a K solamente necesitamos, dada α, preguntar si la palabra $h\ q_0\ \alpha\ h$ es elemento de E, usando el resultado (todavía no demostrado del todo) de que T para con entrada α si y sólo si $h\ q_0\ \alpha\ h$ es equivalente a $h\ q'\ h$. Pero no existe ningún algoritmo para decidir la pertenencia a K, ya que K no es recursivo. Así pues, la hipótesis de que $\mathscr{S}$ tenga un problema de palabras recursivamente soluble lleva a contradicción, y la proposición queda demostrada, supuesto el siguiente lema:

Lema: T para con entrada α si y sólo si las palabras $h\ q_0\ \alpha\ h$ y $h\ q'\ h$ son equivalentes.

Demostración: Supongamos que $h\ q_0\ \alpha\ h$ y $h\ q'\ h$ son equivalentes. Vamos a demostrar que T para con entrada α (el otro sentido de la implicación ya se ha demostrado en la discusión que precede a la proposición). Una demostración de que las palabras son equivalentes consistiría en una transformación, usando las relaciones 1 a 7, que partiese de $h\ q_0\ \alpha\ h$ y terminase en $h\ q'\ h$. Ahora bien, q' no puede introducirse más que por medio de una aplicación de 7. Se deduce que $h\ q_0\ \alpha\ h$ es equivalente a una palabra en la que aparece el símbolo q. Pero q solamente puede introducirse mediante una aplicación de 4. En una sucesión finita de palabras equivalentes que lleve de $h\ q_0\ \alpha\ h$ a $h\ q'\ h$, consideremos entonces el primer lugar donde se aplica la relación 4. Hasta aquí, cada transformación tiene que haber correspondido a un paso de máquina de Turing (siendo una aplicación de 1, 2 ó 3). Tenemos pues

$$h\ q_0\ \alpha\ h \text{ equivalente a (por ejemplo) } h\ P\ q_i\ X\ Q\ h$$

siendo $P\ q_i\ X\ Q$ la descripción instantánea de la condición de la máquina de Turing alcanzada desde la condición inicial $q_0\ \alpha$. Como 4 se ha aplicado en este punto, $q_i\ X$ no puede aparecer en ninguna cuádrupla de T, de manera que T para cuando alcanza $P\ q_i\ X\ Q$. Así pues, T para con entrada α.

Proposición 7.38

El problema de palabras para semigrupo es recursivamente insoluble.

Demostración: Si existiese un algoritmo que decidiese, para todo semigrupo finitamente presentado S y palabras cualesquiera W_1 y W_2 de S si éstas son o no equivalentes, este algoritmo podía usarse para el semigrupo $\mathscr{S}$, contradiciendo la proposición anterior.

▷ Hemos obtenido, pues, los resultados que deseábamos para semigrupos.

Definición 7.39

Un *grupo finitamente presentado* se define análogamente a un semigrupo finitamente presentado, excepto que en las palabras pueden aparecer inversos formales (es decir, las palabras están construidas a partir de los símbolos $a_1, a_2, \ldots, a_k, a_1^{-1}, \ldots, a_k^{-1}$), y que entre las relaciones deben figurar siempre $a_i\, a_i^{-1} = e$ para $1 \leqslant i \leqslant k$, donde e denota la palabra vacía.

Con esta situación, obviamente más complicada, el problema de palabras es más difícil, y la respuesta sólo se ha encontrado hace relativamente poco.

Proposición 7.40

(i) Existe un grupo finitamente presentado cuyo problema de palabras es recursivamente insoluble.

(ii) El problema de palabras para grupos es recursivamente insoluble.

(iii) El problema de palabras para grupos *abelianos* es recursivamente *soluble*. (Para un grupo abeliano finitamente presentado, el conjunto de relaciones debe incluir $a_i\, a_j = a_j\, a_i$ para cada par de símbolos a_i, a_j del alfabeto.

Ejercicios

19 En cada uno de los casos de más abajo, descríbase un algoritmo para resolver el problema de palabras del semigrupo finitamente generado cuyos generadores y relaciones son los dados.
(*a*) $\{a_1, a_2\}$, $a_1\, a_1 = a_1$.
(*b*) $\{a_1, a_2, a_3\}$, $a_2\, a_2 = a_2$, $a_1 a_2 = a_3$.
(*c*) $\{a_1, a_2, a_3, a_4\}$, $a_1 a_1 = e$, $a_2 a_2 = e$, $a_3 a_3 = e$, $a_4 a_4 = e$.

20 Sea G el grupo finitamente presentado de generadores $\{a_1, a_2, a_3\}$ y relaciones $a_1 a_2 = a_2 a_1$, $a_2 a_3 = a_3 a_2$, $a_3 a_1 = a_1 a_3$. Demuéstrese que el problema de palabras para G es recursivamente soluble.

21 Sea S un semigrupo finitamente presentado con problema de palabras recursivamente insoluble. Sea A el conjunto de generadores de S. Demuéstrese que S' tiene un problema de palabras recursivamente insoluble, siendo S' cualquier semigrupo finitamente presentado cuyo conjunto de generadores incluya a A y cuyo conjunto de relaciones sea el mismo S.

22 Dedúzcase del resultado de la Proposición 7.37 que existe un semigrupo finitamente presentado con sólo dos generadores, que tiene un problema de palabras recursivamente insoluble.

7.4. Indecibilidad de sistemas formales

El lector recordará el resultado del Capítulo 2 (Proposición 2.24) de que el sistema formal L del cálculo proposicional es *decidible*. Natural-

mente, entonces ello significaba para nosotros menos que ahora, puesto que ahora podemos demostrar:

Proposición 7.41

El conjunto de los números de Gödel de teoremas de L es un conjunto recursivo.

Demostración: Nótese primero que para L hemos de definir una nueva numeración de Gödel, ya que L no tiene los mismos símbolos que nuestros lenguajes de primer orden $\mathscr{L}$. Esto no presenta ninguna dificultad, ya que L es más sencillo. Por ejemplo, a (y a) se les pueden asignar los números 3 y 5 como antes, a $\sim$ y a $\rightarrow$ pueden asignárseles 7 y 9 respectivamente, y a cada letra de enunciado p_k puede asignársele el número $9+2k$, para $k=1, 2, \ldots$ A las *fbfs.* y sucesiones finitas de *fbfs.* se les asignan entonces números del mismo modo que antes, usando potencias de primos.

Para demostrar la proposición necesitamos un algoritmo que responda a preguntas del conjunto

$$\{\text{¿es } n \text{ el número de Gödel de un teorema de } L?/n \in D_N\}$$

Dado $n \in D_N$, encuéntrese la *fbf.* de L correspondiente a L (si hay alguna). Si no hay ninguna, la respuesta requerida es «no», Si hay una, se construye su tabla de verdad y se observa si la *fbf.* es una tautología o no.

▷ El problema de la decidibilidad o indecibilidad recursiva puede plantearse de hecho a cualquiera de nuestros sistemas formales, ya que la idea de numeración de Gödel se aplica a todos ellos. El problema se reduce entonces al de la recursividad o no recursividad de un subconjunto de D_N.

El si el sistema $K_{\mathscr{L}}$ del cálculo de predicados es o no recursivamente indecible, depende del leguaje $\mathscr{L}$. Para tomar un caso extremo, sea $\mathscr{L}_1$ el lenguaje de primer orden que no contiene letras de función ni constantes individuales, y que contiene una sola letra de predicado A_1^1.

Proposición 7.42

$K_{\mathscr{L}_1}$ es recursivamente decidible.

Demostración: Vamos a describir un algoritmo para responder a preguntas del conjunto

$$\{\text{¿es } \mathscr{A} \text{ un teorema de } K_{\mathscr{L}_1}?/\mathscr{A} \textit{ fbf.} \text{ de } K_{\mathscr{L}_1}\}$$

Para hacerlo, vamos a utilizar el resultado del Capítulo 4 de que una

fbf. $\mathscr{A}$ es un teorema de $K_{\mathscr{L}_1}$ si y sólo si $\mathscr{A}$ es verdadera en toda interpretación de $\mathscr{L}_1$.

Sea I una interpretación de $\mathscr{L}_1$. Entonces, $D_I = D_0 \cup D_1$, siendo

$$D_0 = \{x \in D_I : \bar{A}_1^1(x) \text{ se verifica}\}$$

y

$$D_1 = \{x \in D_I : \bar{A}_1^1(x) \text{ no se verifica}\}$$

(Nótese que D_0 o D_1 puede ser vacío, pero no ambos simultáneamente.)

Definimos ahora una interpretación I^* como sigue. El dominio de I^* es $\{D_0, D_1\}$ si D_0 y D_1 son ambos no vacíos, o $\{D_0\}$ si $D_1 = \varnothing$, o $\{D_1\}$ si $D_0 = \varnothing$. La interpretación de A_1^1 es, pongamos $\bar{A}_1^1$, teniéndose que $\bar{A}_1^1(D_0)$ se verifica y $\bar{A}_1^1(D_1)$ no se verifica. Para toda *fbf.* $\mathscr{A}$ de $\mathscr{L}_1$, si $\mathscr{A}$ es verdadera en I^*, entonces $\mathscr{A}$ es verdadera en I. Esto se demuestra por inducción sobre el número de conectivas y cuantificadores de $\mathscr{A}$, pero nótese que se requieren demostraciones diferentes para los diferentes casos, según I^* tenga dominio $\{D_0\}$, $\{D_0, D_1\}$ o $\{D_1\}$.

Se deduce de lo anterior que si una *fbf.* $\mathscr{A}$ es verdadera en toda interpretación cuyo dominio contenga a lo sumo dos elementos, entonces $\mathscr{A}$ es verdadera en todas las interpretaciones. Nuestro algoritmo, pues, debe ser un método para comprobar si una *fbf.* es verdadera en toda interpretación cuyo dominio conste de uno o dos elementos. Toda interpretación de este tipo forzosamente caerá en una de las categorías siguientes:

1. Dominio $\{d\}$, verificándose $\bar{A}_1^1(d)$.
2. Dominio $\{d\}$, no verificándose $\bar{A}_1^1(d)$.
3. Dominio $\{d_1, d_2\}$, verificándose $\bar{A}_1^1(d_1)$ y no verificándose $\bar{A}_1^1(d_2)$.
4. Dominio $\{d_1, d_2\}$, verificándose $\bar{A}_1^1(d_1)$ y $\bar{A}_1^1(d_2)$.
5. Dominio $\{d_1, d_2\}$, no verificándose ni $\bar{A}_1^1(d_1)$ ni $\bar{A}_1^1(d_2)$.

Para cualquier *fbf* dada $\mathscr{A}$, es fácil comprobar si $\mathscr{A}$ es verdadera en las interpretaciones de cualquiera de estas categorías, usando los métodos del Capítulo 3.

Este algoritmo puede usarse para decidir si una *fbf* arbitraria dada es un teorema, así que $K_{\mathscr{L}_1}$ es recursivamente decidible.

▷ Las ideas de la demostración anterior pueden extenderse, dando el resultado mucho más general:

Proposición 7.43

Sea $\mathscr{L}$ un lenguaje de primer orden que no contiene ni letras de función ni constantes individuales, y que contiene solamente letras de pre-

dicado de un argumento (eventualmente una lista infinita de ellas). Entonces $K_{\mathscr{L}}$ es recursivamente decidible.

Demostración: Véase Mendelson.

▷(Un sistema tal como el $K_{\mathscr{L}}$ descrito más arriba se llama a menudo sistema de cálculo de predicados de primer orden *puro*, indicando la ausencia de letras de función y constantes individuales).

En contraste con la anterior, tenemos la proposición siguiente:

Proposición 7.44

El sistema $\mathscr{N}$ es recursivamente indecidible (bajo la hipótesis de que sea consistente).

Demostración: Sea T una relación monaria sobre D_N definida por: $T(n)$, se verifica si y sólo si n es el número de Gödel de un teorema de $\mathscr{N}$. Supongamos que T es recursiva (es decir, que $\mathscr{N}$ es recursivamente decidible). Entonces, por la Proposición 6.12, T es expresable en $\mathscr{N}$, y por tanto existe una *fbf*, $\mathscr{T}(x_1)$ en la que x_1 aparece libre, tal que

$$\text{si } T(n) \text{ se verifica, entonces } \vdash_{\mathscr{N}} \mathscr{T}(0^{(n)}),$$

y

$$\text{si } T(n) \text{ no se verifica, entonces } \vdash_{\mathscr{N}} \sim\mathscr{T}(0^{(n)}).$$

Sea D la relación binaria sobre D_N definida por: $D(m,n)$ se verifica si y sólo si se tiene uno de los dos casos: m es el número de Gödel de una *fbf* $\mathscr{A}(x_1)$ en la que x_1 aparece libre, y n es el número de Gödel de $\mathscr{A}(0^{(m)})$, o m no es el número de Gödel de una *fbf* así y $n=0$. Entonces, D es una función recursiva y por tanto representable en $\mathscr{N}$ (véase la Proposición 6.29). Supongamos que la *fbf* $\mathscr{D}(x_1,x_2)$ la representa.

Denotaremos por $\mathscr{A}(x_1)$ la *fbf*

$$(\forall x_2)(\mathscr{D}(x_1,x_2)\rightarrow\sim\mathscr{T}(x_2)).$$

Sea s el número de Gödel de esta *fbf*. Entonces $\mathscr{A}(0^{(s)})$ es la *fbf*

$$(\forall x_2)(\mathscr{D}(0^{(s)},x_2)\rightarrow\sim\mathscr{T}(x_2)).$$

Sea t el número de Gödel de esta *fbf*. Entonces se verifica $D(s,t)$, y con ello $\vdash_{\mathscr{N}} \mathscr{D}(0^{(s)},0^{(t)})$. Ahora bien, si $\mathscr{A}(0^{(s)})$ es un teorema de $\mathscr{N}$, obtenemos usando el axioma $(K5)$

$$\vdash_{\mathscr{N}} (\mathscr{D}(0^{(s)},0^{(t)})\rightarrow\sim\mathscr{T}(0^{(t)})).$$

Se deduce que

$$\vdash_{\mathscr{N}} \sim\mathscr{T}(0^{(t)}), \text{ por } MP.$$

Además, si $\mathscr{A}(0^{(s)})$ no es teorema de $\mathscr{N}$, entonces t no es el número de Gödel de ningún teorema de $\mathscr{N}$, así que $T(t)$ no se verifica, con lo cual $\vdash_{\mathscr{N}} \sim \mathscr{T}(0^{(t)})$. Así pues, tenemos en todo caso

$$\vdash_{\mathscr{N}} \sim \mathscr{T}(0^{(t)})$$

Ahora bien

$$\vdash_{\mathscr{N}} \mathscr{D}(0^{(s)}, 0^{(t)}),$$

y como D es representable en $\mathscr{N}$, tenemos

$$\vdash_{\mathscr{N}} (\exists_1 x_2)\, \mathscr{D}(0^{(s)}, x_2).$$

Así pues

$$\vdash_{\mathscr{N}} (\mathscr{D}(0^{(s)}, x_2) \rightarrow x_2 = 0^{(t)}). \qquad (*)$$

Nuestros axiomas para la igualdad nos proporcionan

$$\vdash_{\mathscr{N}} (x_2 = 0^{(t)} \rightarrow (\sim \mathscr{T}(0^{(t)}) \rightarrow \sim \mathscr{T}(x_2))),$$

y como $\vdash_{\mathscr{N}} \sim \mathscr{T}(0^{(t)})$, tenemos

$$\vdash_{\mathscr{N}} (x_2 = 0^{(t)} \rightarrow \sim \mathscr{T}(x_2)).$$

Con ayuda de (*) y usando la regla (SH) obtenemos

$$\vdash_{\mathscr{N}} (\mathscr{D}(0^{(s)}, x_2) \rightarrow \sim \mathscr{T}(x_2)),$$

y por Generalización

$$\vdash_{\mathscr{N}} (\forall x_2)(\mathscr{D}(0^{(s)}, x_2) \rightarrow \sim \mathscr{T}(x_2)),$$

es decir,

$$\vdash_{\mathscr{N}} \mathscr{A}(0^{(s)}).$$

Así pues, t es el número de Gödel de un teorema de $\mathscr{N}$, así que

$$\vdash_{\mathscr{N}} \mathscr{A}(0^{(s)}).$$

Pero $\vdash_{\mathscr{N}} \sim \mathscr{T}(0^{(t)})$, de manera que esto contradice la consistencia de $\mathscr{N}$. Hemos completado la demostración.

▷ Si se sabe que un sistema es recursivamente decidible (o indecidible), ¿podemos deducir algo acerca de la decidibilidad (o indecidibilidad) recursiva de extensiones suyas? Recuérdese que una extensión de un sistema de primer orden tiene el mismo lenguaje, pero una clase más extensa de teoremas. En vista de esto, podría parecer que no hay razón para que la existencia (o no existencia) de un algoritmo que decide la pertenencia a una de las clases de teoremas implique la existencia (o no existencia) de un algoritmo que decida la pertenencia a la otra. (Un

conjunto recursivo puede tener un subconjunto no recursivo, y un conjunto no recursivo puede tener un subconjunto recursivo.) No obstante, en ciertas circunstancias puede establecerse una conexión.

Proposición 7.45

Sea S y S^+ sistemas de primer orden con el mismo lenguaje, y sea S^+ una extensión *finita* de S, es decir, supongamos que exista un conjunto finito $\mathscr{A}_1, \ldots, \mathscr{A}_n$ de *fbfs.* tales que añadiéndolas a los axiomas de S se obtiene un conjunto de axiomas para S^+. Si S^+ es recursivamente indecidible, entonces S es también recursivamente indecidible.

Demostración: Supongamos que S y S^+ son como los hemos descrito, y que S^+ es recursivamente indecidible. Sin pérdida de la generalidad podemos suponer que $\mathscr{A}_1, \ldots, \mathscr{A}_n$ son *fbfs* cerradas. Una demostración en S^+ es una deducción en S a partir de $\{\mathscr{A}_1, \ldots, \mathscr{A}_n\}$ de manera que para toda *fbf.* $\mathscr{A}$,

$$\vdash_{S^+} \mathscr{A} \text{ si y sólo si } \vdash_S (\mathscr{A}_1 \rightarrow (\ldots \rightarrow (\mathscr{A}_n \rightarrow \mathscr{A}))\ldots)$$

usando el Teorema de Deducción. Si existiese un algoritmo para decidir si cualquier *fbf.* dada es un teorema de S, podríamos decidir si cualquier *fbf.* $\mathscr{A}$ dada es un teorema de S^+ sin más que preguntar si $(\mathscr{A}_1 \rightarrow (\ldots \rightarrow (\mathscr{A}_n \rightarrow \mathscr{A}\cdots)$ es un teorema de S. Pero S^+ es recursivamente indecidible y, por tanto, S debe ser también recursivamente indecidible.

▷ Resumiendo: Hemos descubierto dos limitaciones del sistema $\mathscr{N}$: No es completo y es recursivamente indecidible. En primer lugar, el conjunto de los teoremas de $\mathscr{N}$ no coincide con el conjunto de los enunciados verdaderos, y en segundo lugar, no existe ningún algoritmo para decidir qué enunciados corresponden a teoremas de $\mathscr{N}$. Podría parecer, pues, que $\mathscr{N}$ no ayuda mucho a proporcionar un método para decidir la verdad o falsedad de enunciados aritméticos. Los sistemas formales en este libro, sufren estas limitaciones, y hasta ahora hay enfoques alternativos conocidos.

Otro resultado importante es (cfr. Proposición 7.42).

Proposición 7.46

Existe un lenguaje de primer orden $\mathscr{L}$ tal que $K_{\mathscr{L}}$ es recursivamente indecidible.

Demostración: La demostración hace uso de ideas similares a las de la demostración de la Proposición 7.37. Sea T una máquina de Turing que pare si y sólo si el número de entrada pertenece al conjunto K (que es recursivamente enumerable pero no recursivo). Supongamos

que T use 1 y B como únicos símbolos de cinta, y que sus estados internos sean $q_0, \ldots, q_n$. Sea ahora $\mathscr{L}$ un lenguaje de primer orden cuyo alfabeto de símbolos incluya como constantes individuales todos los símbolos del conjunto

$$A = \{B,\ 1,\ h,\ q,\ q',\ q_o,\ \ldots,\ q_n\}$$

y que incluya también la letra de función f_2^2 y la letra de predicado A_2^2. Imaginaremos que f_2^2 nos permite formar palabras, es decir, $f_2^2(x_1,x_2)$ ha de imaginarse como la palabra x_1x_2. Los términos de $\mathscr{L}$ corresponderán entonces a palabras de longitud cualquiera (permitiendo que intervengan variables) y el conjunto de todos los términos cerrados de $\mathscr{L}$ en los que intervengan exclusivamente los símbolos de A y la letra f_2^2 corresponderá al conjunto S_A. (Cualquier palabra dada corresponderá a varios términos diferentes, debido a las distintas disposiciones posibles de los paréntesis, pero esto ya lo tendremos en cuanta en lo que sigue.)

La letra de predicado A_2^2 ha de imaginarse como la relación de equivalencia sobre S_A generada por las relaciones que enumeramos para el semigrupo con problema de palabra insoluble descrito en la demostración de la Proposición 7.37.

Las características de f_2^2 y A_2^2 han de ser descritas, y esto es lo que hacen las siguientes *fbfs.* de $K_{\mathscr{L}}$.

(I1) $A_2^2(f_2^2(f_2^2(x_1,\ x_2),\ x_3),\ f_2^2(x_1,\ f_2^2(x_2,\ x_3)))$.

(I2) $A_2^2(x_1,\ x_2) \rightarrow A_2^2(f_2^2(x_1,\ x_3),\ f_2^2(x_2,\ x_3))$.

(I3) $A_2^2(x_1,\ x_2) \rightarrow A_2^2(f_2^2(x_3,\ x_1),\ f_2^2(x_3,\ x_2))$.

(I4) Para cada relación $W = W'$ del conjunto de relaciones que determinan el semigrupo con problema de palabras insoluble, obtenemos términos cerrados t,t' de $K_{\mathscr{L}}$ correspondientes a las palabras W y W' e incluimos como (I4) todas las *fbfs.*

$$A_2^2(t,\ t')$$

obtenidas de este modo. Nótese que sólo hay un número finito de ellas.

(I5) $A_2^2(x_1,\ x_2) \rightarrow (A_2^2(x_2,\ x_3) \rightarrow A_2^2(x_1,\ x_3))$.

Si consideramos el sistema de primer orden $K_{\mathscr{L}}^*$ obtenido a partir de $K_{\mathscr{L}}$ incluvendo todas las *fbfs.* (I1)–(I5) como nuevos axiomas, debería resultar claro que para términos cerrados cualesquiera t_1, t_2 de $\mathscr{L}$ correspondientes a palabras W_1, W_2 de S_A, tenemos

$$\vdash_{K_{\mathscr{L}}^*} A_2^2(t_1,t_2) \text{ si y sólo si } W_1 \text{ y } W_2 \text{ son equivalentes}$$

En particular,

$$\vdash_{K^*_{\mathscr{L}}} A_2^2(t_1 f_2^2(h, f_2^2(q', h))) \text{ si y sólo si } W_1 \text{ es equivalente a } hq'h.$$

Supongamos ahora que $K^*_{\mathscr{L}}$ fuese recursivamente decidible, es decir, que existiese un algoritmo para decidir, para cualquier *fbf.* $\mathscr{A}$, si $\vdash_{K^*_{\mathscr{L}}} \mathscr{A}$. Dada entonces una palabra $W \in S_A$, para decidir si W es equivalente a $h\ q'\ h$ en S_A todo lo que necesitamos hacer es formar la *fbf.* $A_2^2(t, f_2^2(h, f_2^2(q', h)))$ (donde t corresponde a W) y preguntar si es un teorema de $K^*_{\mathscr{L}}$. Tenemos pues un algoritmo para decidir, para toda palabra W de S_A, si ésta es equivalente a $h\ q'\ h$, y esto contradice nuestro anterior resultado. Así pues, $K^*_{\mathscr{L}}$ es recursivamente indecidible. Pero $K^*_{\mathscr{L}}$ es una extensión finita de $K_{\mathscr{L}}$ (ya que (I1)-(I5) constituyen un conjunto finito de *fbfs.*). Por la Proposición 7.45, $K_{\mathscr{L}}$ es entonces recursivamente indecidible.

▷ El lector debería cuidar de guardar este resultado en el contexto de la Proposición 7.42, y recordar que el si un sistema de cálculo de predicados es recursivamente decidible o indecidible depende del lenguaje $\mathscr{L}$. No obstante, debería observarse que la indecidibilidad es la regla más bien que la excepción, y de hecho la demostración anterior puede modificarse fácilmente para demostrar que si $\mathscr{L}$ contiene por lo menos una letra de función de dos argumentos, por lo menos una letra de predicado de dos argumentos, y una lista infinita de constantes individuales, entonces $K_{\mathscr{L}}$ es recursivamente indecidible.

Corolario 7.47

El cálculo de predicados de primer orden entero (con todos los símbolos indicados en el Capítulo 3) es recursivamente indecidible.

▷ Finalicemos con algunos ejemplos que indican que para sistemas matemáticamente significativos, la indecidibilidad recursiva es lo más usual.

Proposición 7.48

(i) Los siguientes sistemas son recursivamente indecidibles.
  (*a*) Teoría de grupos de primer orden.
  (*b*) Teoría de anillos de primer orden.
  (*c*) Teoría de cuerpos de primer orden.
  (*d*) Teoría de semigrupos de primer orden.
  (*e*) El sistema *ZF*.

(ii) Los siguientes sistemas son recursivamente decidibles.

(*a*) Teoría de primer orden de grupos *abelianos*.
(*b*) Aritmética de primer orden sin multiplicación (es decir, el sistema que coincide con $\mathcal{N}$ salvo en que el símbolo f_2^2 no se incluye, y los axiomas $(N5)$ y $(N6)$ se omiten).

Demostración: No vamos a entrar en las demostraciones, pero referimos al lector interesado al libro de Tarski, Mostowski y Robinson.

▷ La decidibilidad recursiva de un sistema formal implica la existencia de un programa de computador que decidirá, dada cualquier *fbf* del sistema, si es un teorema o no (suponiendo que el computador sea lo suficientemente grande, por supuesto). Así pues, es posible decidir, por ejemplo, usando una máquina y un solo programa, qué enunciados referentes a grupos abelianos y sus elementos son teoremas y cuáles no. Un programa así sería excesivamente complejo, y las decisiones referentes a enunciados complicados requerirían una cantidad considerable de tiempo y capacidad del computador, de modo que esto no es útil en un sentido práctico, pero la posibilidad es interesante. Asimismo lo es la imposibilidad de encontrar un programa análogo para la teoría de grupos y los otros sistemas enumerados más arriba como recursivamente indecidibles. En particular, la indecidibilidad de ZF implica que no existe ningún programa universal que pueda usarse para decir si los enunciados matemáticos en general son teoremas o no. ¡Puede ser que los computadores den la vuelta al mundo, pero nunca podrán reemplazar a los matemáticos!

Ejercicios

23 (Véase la Proposición 7.42). Sea $\mathcal{L}_2$ el lenguaje de primer orden sin constantes individuales ni letras de función, y con sólo dos letras de predicado de un argumento A_1^1 y A_2^1. Demuéstrese que una *fbf* $\mathscr{A}$ de $\mathcal{L}_2$ es verdadera en toda interpretación si es verdadera en toda interpretación cuyo dominio contenga cuatro o menos elementos. Descríbase un algoritmo para decidir si una *fbf* $\mathscr{A}$ de $\mathcal{L}_2$ es verdadera en toda interpretación así.

24 Demuéstrese que los siguientes conjuntos no son recursivos.
(*a*) $\{n \in D_N : n$ es el número de Gödel de una *fbf* $\sim\mathscr{A}$, siendo $\mathscr{A}$ un teorema de $\mathcal{N}\}$.
(*b*) $\{n \in D_N : n$ es el número de Gödel de una *fbf* $\mathscr{A}$ de $\mathcal{N}$ falsa en $N\}$.
(c) $\{n \in D_N : n$ es el número de Gödel de una *fbf* $\mathscr{A}$ de $\mathcal{N}$ que no es un teorema de $\mathcal{N}\}$.

25 De los conjuntos dados en el Ejercicio 24, demuéstrese que (i) es recursivamente enumerable y que (iii) no es recursivamente enumerable.

26 Demuéstrese que el conjunto (ii) del Ejercicio 24 no es recursivamente enumerable, del modo siguiente. Supongamos por el contrario que el conjunto es enumerado por la función recursiva f. Definamos una relación F sobre D_N poniendo: $F(m, n)$ se cumple si y sólo si m es el número de

Gödel de $\mathscr{A}(0^{(m)})$. Demuéstrese que F es recursiva (usando la Tesis de Church). Entonces F es representable en $\mathscr{N}$, mediante la *fbf* $\mathscr{F}(x_1, x_2)$, pongamos. Sea ahora p el número de Gödel de la *fbf* $(\exists x_2)\mathscr{F}(x_1, x_2)$, y sea $\mathscr{V}$ la *fbf* $(\exists x_2)\mathscr{F}(0^{(p)}, x_2)$. Demuéstrese que $\mathscr{V}$ es falsa en N y que el número de Gödel de $\mathscr{V}$ no está en el rango de f, lo que es una contradicción. (Cf. la demostración del Teorema de Incompletitud de Gödel en la Sección 6.5.)

27 Digamos que un sistema de primer orden S es *recursivamente axiomatizable* si existe un sistema de primer orden T que tiene los mismos teoremas que S, tal que el conjunto de los números de Gödel de los axiomas de T es recursivo. Demuéstrese que si S es recursivamente axiomatizable, entonces el conjunto de los números de Gödel de los teoremas de S es recursivamente enumerable. Dedúzcase que si S es recursivamente axiomatizable y completo, entonces S es recursivamente decidible.

Apéndice. Conjuntos numerables y no numerables

Definición A1

Un conjunto es *numerable* si puede ponerse en correspondencia biunívoca con el conjunto de los números naturales. En otras palabras, un conjunto A es numerable si existe una biyección $f: D_N \to A$.

Nótese que los elementos de un conjunto numerable pueden escribirse en una lista, y que la biyección dada en la definición proporciona un método para hacer esto, concretamente enumera $f(0), f(1), f(2), \ldots$

Trivialmente, los números naturales constituyen un conjunto numerable.

Proposición A2

Si A y B son conjuntos numerables, entonces existe una biyección entre A y B. Recíprocamente, si A es un conjunto numerable y existe una biyección entre A y B, entonces B es numerable.

Demostración: Sean $f: D_N \to A$ y $g: D_N \to B$ biyecciones. Entonces $g \circ f^{-1}$ es una biyección de A en B.

Recíprocamente, sea $f: D_N \to A$ una biyección, de modo que A sea numerable, y supongamos que existe una biyección h de A en B. Entonces $h \circ f$ es una biyección de D_N en B, y así B es numerable.

Proposición A3

Todo subconjunto infinito de un conjunto numerable es numerable.

Demostración: Sea A un conjunto numerable, sea $f: D_N \to A$ una biyección y sea B un subconjunto infinito de A. Entonces $f(0), f(1), f(2), \ldots$ es una lista de todos los elementos de A. Borremos de esta lista todos los elementos que no pertenezcan a B. Lo que queda es una lista (infinita) de los elementos de B. Una biyección $g: D_N \to B$ puede definirse ahora poniendo

$$g(n) = \text{el } (n+1)\text{-ésimo miembro de la nueva lista } (n \in D_N)$$

(Ha de ser el $(n+1)$-ésimo miembro porque $g(0)$ es el primero, $g(1)$ es el segundo, y así sucesivamente.)

Proposición A4

Un conjunto infinito A es numerable si y sólo si existe una inyección $h: A \to D_N$.

Demostración: Si A es numerable entonces existe una biyección $D_N \to A$, cuya inversa es ciertamente una inyección $A \to D_N$.
Recíprocamente, supongamos que existe una inyección $h: A \to D_N$. $h(A) \subseteq D_N$ y $h(A)$ es infinito, pues h es inyectiva. Por la Proposición A3, $h(A)$ es numerable. Sea $g: D_N \to h(A)$ una biyección. La composición $h^{-1} \circ g$ es entonces una biyección de D_N en A, y A es numerable.

▷ Este último resultado suele ser el que más conviene utilizar en una demostración de que un conjunto particular es numerable, y en seguida veremos aplicaciones suyas.

Proposición A5

La unión de dos conjuntos numerables disjuntos es numerable.

Demostración: Sean A y B los conjuntos numerables disjuntos y sean $f: D_N \to A$ y $g: D_N \to B$ las biyecciones. Definamos $h: D_N \to A \cup B$ como sigue:

$$h(n) = \begin{cases} f\left(\frac{1}{2}n\right) & \text{si } n \text{ es par} \\ f\left(\frac{1}{2}n - \frac{1}{2}\right) & \text{si } n \text{ es impar} \end{cases}$$

Corolario A6

La unión de cualquier colección finita de conjuntos numerables disjuntos es numerable.

Demostración: La demostración es por inducción sobre el número de conjuntos de la colección.

Paso base: La unión de dos conjuntos numerables disjuntos es numerable, por la proposición.

Paso de inducción: Sea $n > 2$ y sean $A_1, \ldots, A_n$ conjuntos numerables disjuntos. Supongamos como hipótesis de inducción que una unión de $n-1$ conjuntos numerables disjuntos es numerable. Entonces $A_1 \cup A_2 \cup \ldots \cup A_{n-1}$ es numerable (y disjunto de A_n). Por la proposición se tiene entonces que el conjunto $(A_1 \cup A_2 \cup \ldots \cup A_{n-1}) \cup A_n$ es numerable.

El resultado se deduce del principio de inducción matemática.

Observación: Puede prescindirse de la hipótesis de que los conjuntos sean disjuntos. Una demostración de esto se deja como ejercicio para el lector.

Problema: ¿Existen conjuntos que no sean ni finitos ni numerables? Sabemos por lo anterior que D_N y todos sus subconjuntos son finitos o numerables. La respuesta se da en la siguiente proposición.

Proposición A7

El conjunto de todos los subconjuntos de D_N es infinito y no numerable.

Demostración: Denotemos por $P(D_N)$ al conjunto de todos los subconjuntos de D_N. $P(D_N)$ es claramente infinito. Supongamos que fuese numerable y sea $f: D_N \to P(D_N)$ una biyección. Entonces, para cada $n \in D_N$, $f(n)$ es un subconjunto de D_N. Sea

$$B = \{k \in D_N : k \notin f(k)\}$$

B es desde luego un subconjunto de D_N (que podría eventualmente ser vacío o ser todo D_N). Además $B \neq f(n)$ para todo $n \in D_N$. En efecto, supongamos que $B = f(n)$. Si $n \in f(n)$, entonces $n \in B$, pues $B = f(n)$, pero $n \notin B$ por definición de B. Si $n \notin f(n)$, entonces $n \notin B$, pues $B = f(n)$, pero $n \in B$ por definición de B. En ambos casos llegamos a una contradicción. Así pues, $B \neq f(n)$ para todo $n \in D_N$, y con ello f no es una biyección entre D_N y $P(D_N)$. Esto contradice nuestra suposición original, y por tanto $P(D_N)$ no es numerable.

Corolario A8

El conjunto de todas las funciones sobre D_N es no numerable.

Demostración: Para cada subconjunto A de D_N, definimos una función $C_A: D_N \to D_N$ (la función característica de A) como sigue:

$$C_A(n) = \begin{cases} 0 \text{ si } n \in A \\ 1 \text{ si } n \notin A \end{cases}$$

La correspondencia entre conjuntos A y funciones C_A es una biyección entre $P(D_N)$ y un *subconjunto* del conjunto de las funciones sobre D_N. $P(D_N)$ no es numerable, de modo que el conjunto de las funciones sobre D_N tiene un subconjunto que no es numerable. (Si existe una biyección entre dos conjuntos y uno de ellos es numerable, entonces el otro es numerable). Si el conjunto de las funciones sobre D_N fuese numerable, entonces todo subconjunto infinito suyo sería numerable (Proposi-

ción A3). Así pues, por tener un subconjunto no numerable, el conjunto de todas las funciones sobre D_N es no numerable.

Corolario A9

El conjunto de todas las relaciones sobre D_N es no numerable.

Demostración: El conjunto de las relaciones contiene al conjunto de las funciones. Por una argumentación similar a la anterior se tiene entonces que el conjunto de las relaciones no puede ser numerable.

▷ En el texto usamos el resultado de que si un conjunto no numerable tiene un subconjunto numerable, entonces el subconjunto debe ser propio. Esto debería estar claro ahora, ya que un conjunto no puede ser a la vez numerable y no numerable.

Usamos también el resultado de que el conjunto de las *fbfs* de un lenguaje simbólico dado era numerable. Hay algunos resultados generales que nos llevan a ver por qué esto es así.

Proposición A10

Sea A un conjunto numerable. La colección de todos los subconjuntos finitos de A es un conjunto numerable.

Demostración: Sea f: $D_N \rightarrow A$ una biyección. Podemos definir una inyección g del conjunto de todos los subconjuntos finitos de A en D_N como sigue. Sea F un subconjunto finito de A. Entonces $f^{-1}(F)$ es un subconjunto finito de D_N. Sea $g(F)$ = el producto de los primos p_n, para $n \in f^{-1}(F)$. (Aquí p_i denota el i-ésimo primo impar, para $i > 0$, y $p_0 = 2$.) g es inyectiva, porque un mismo producto de primos no puede surgir de dos conjuntos F distintos, y dos productos de primos diferentes no pueden ser iguales. Por la Proposición A4 se tiene entonces que el conjunto de todos los subconjuntos finitos de A es numerable.

Proposición A11

Sea A un conjunto numerable. Entonces el conjunto de todas las *sucesiones* finitas de elementos de A es un conjunto numerable.

Demostración: Aquí podemos hacer uso de las propiedades de los números primos de manera ligeramente distinta. Sea f: $D_N \rightarrow A$ una biyección. Definimos una inyección h del conjunto de todas las sucesiones finitas de elementos de A en D_N así. Si $u_0, u_1, \ldots, u_k \in A$, sea

$$h(u_0, u_1, \ldots, u_k) = p_0^{f^{-1}(u_0)} \times p_1^{f^{-1}(u_1)} \times \cdots \times p_k^{f^{-1}(u_k)},$$

siendo los p_i como en la demostración anterior. h es inyectiva porque f es una biyección y por la unicidad de la descomposición en factores

primos. Por la Proposición A4 se tiene entonces que el conjunto de todas las sucesiones finitas de elementos de A es numerable.

▷ Esta proposición tiene como corolario el resultado que necesitamos acerca de lenguajes formales. Todos nuestros lenguajes formales tienen como alfabeto de símbolos un conjunto numerable. (La demostración de esto requiere el uso del Corolario A6). El conjunto de las *fbfs* de lenguaje formal $\mathscr{L}$ es un subconjunto del conjunto de todas las sucesiones finitas de símbolos del alfabeto de $\mathscr{L}$. Este conjunto de sucesiones finitas es numerable, de modo que todo subconjunto suyo es también numerable (o finito). Pero sabemos que el conjunto de todas las *fbfs* es siempre infinito, con lo que tenemos nuestro resultado.

Indicaciones y soluciones de ejercicios seleccionados

Capítulo 1

Sección 1.1 (págs. 11-12)

1(*a*) $(A \wedge B) \rightarrow C$.
(*g*) $A \leftrightarrow (B \vee C)$.
(*h*) $A \rightarrow (B \rightarrow C)$.

Sección 1.2 (pág. 19)

5 (*a*), (*b*), (*d*).
7 Tómese p verdadera y q verdadera. Tómense $\mathscr{A}$ y $\mathscr{B}$ como tautologías cualesquiera.

Sección 1.3 (pág. 24)

10 $((\sim p) \vee q)$ es lógicamente equivalente a $(p \rightarrow q)$, luego $(\sim((\sim p) \vee q)) \vee r)$ es lógicamente equivalente a $(\sim(p \rightarrow q) \vee r)$.

Sección 1.4 (pág. 28)

12(*a*) $((p \wedge q) \vee ((\sim p) \wedge (\sim q)))$.
(*d*) $((p \wedge (\sim q) \wedge (\sim r)) \vee ((\sim p) \wedge q \wedge (\sim r)) \vee ((\sim p) \wedge (\sim q) \wedge (\sim r)))$.
13(*a*) $(((\sim p) \vee (\sim q) \vee r) \wedge (p \vee (\sim q) \vee r) \wedge (p \vee q \vee r))$.

Sección 1.5 (pág. 31)

14(*b*) $((p \vee q) \vee (\sim(r \vee (\sim s))))$.
17(*b*) Considérese una forma enunciativa en la que intervengan las variables de enunciado p y q y las conectivas $\sim$ y $\rightarrow$ tan sólo. Demuéstrese que su tabla de verdad debe contener cuatro *Fs* o cuatro *Vs* o dos *Fs* y dos *Vs*. Una demostración completa requiere una inducción del tipo usado en la Proposición 1.15.
19 Una tabla de verdad así tiene que tener cuatro columnas, y por lo tanto debe ser una de entre dieciséis posibles. Las dieciséis pueden darse todas por conocidas o no adecuadas.

Sección 1.6 (págs. 35-36)

20(*b*) $(p \rightarrow (q \vee r))$, $(\sim r)$; $\therefore ((\sim q) \rightarrow (\sim p))$. Válida.

(*d*) $(p \rightarrow (q \wedge r \wedge s))$, q, $(s \rightarrow r)$; $\therefore s \rightarrow p$. Inválida.

Capítulo 2

Sección 2.1 (págs. 46-47)

1(*b*)	(1)	$(p_1 \rightarrow (p_2 \rightarrow p_3)) \rightarrow (p_1 \rightarrow p_2) \rightarrow (p_1 \rightarrow p_3))$	(*L*2)
	(2)	$((p_1 \rightarrow (p_2 \rightarrow p_3)) \rightarrow ((p_1 \rightarrow p_2) \rightarrow (p_1 \rightarrow p_3))) \rightarrow (((p_1 \rightarrow (p_2 \rightarrow p_3)) \rightarrow (p_1 \rightarrow p_2)) \rightarrow ((p_1 \rightarrow (p_2 \rightarrow p_3)) \rightarrow (p_1 \rightarrow p_3)))$	
	(3)	$((p_1 \rightarrow (p_2 \rightarrow p_3)) \rightarrow (p_1 \rightarrow p_2)) \rightarrow ((p_1 \rightarrow (p_2 \rightarrow p_3)) \rightarrow (p_1 \rightarrow p_3))$	(*L*1)
(*d*)	(1)	$p_2 \rightarrow (p_1 \rightarrow p^2)$	(*L*1)
	(2)	$(p_2 \rightarrow (p_1 \rightarrow p_2)) \rightarrow (p_1 \rightarrow (p_2 \rightarrow (p_1 \rightarrow p_2)))$	(*L*1)
	(3)	$(p_1 \rightarrow (p_2 \rightarrow (p_1 \rightarrow p_2)))$	1, 2 *MP*
2(*b*)	(1)	$(\sim \sim \mathscr{A})$	hipótesis
	(2)	$(\sim \sim \mathscr{A}) \rightarrow ((\sim \sim \sim \sim \mathscr{A}) \rightarrow (\sim \sim \mathscr{A}))$	(*L*1)
	(3)	$(\sim \sim \sim \sim \mathscr{A}) \rightarrow (\sim \sim \mathscr{A})$	1, 2 *MP*
	(4)	$((\sim \sim \sim \sim \mathscr{A}) \rightarrow (\sim \sim \mathscr{A})) \rightarrow ((\sim \mathscr{A}) \rightarrow (\sim \sim \sim \mathscr{A}))$	(*L*3)
	(5)	$(\sim \mathscr{A}) \rightarrow (\sim \sim \sim \mathscr{A})$	3, 4 *MP*
	(6)	$((\sim \mathscr{A}) \rightarrow (\sim \sim \sim \mathscr{A})) \rightarrow ((\sim \sim \mathscr{A}) \rightarrow \mathscr{A})$	(*L*3)
	(7)	$(\sim \sim \mathscr{A}) \rightarrow \mathscr{A}$	5, 6 *MP*
	(8)	$\mathscr{A}$	1, 7 *MP*
(*d*)	(1)	$\mathscr{A} \rightarrow (\mathscr{B} \rightarrow \mathscr{C})$	hipótesis
	(2)	$(\mathscr{A} \rightarrow (\mathscr{B} \rightarrow \mathscr{C})) \rightarrow ((\mathscr{A} \rightarrow \mathscr{B}) \rightarrow (\mathscr{A} \rightarrow \mathscr{C}))$	(*L*2)
	(3)	$(\mathscr{A} \rightarrow \mathscr{B}) \rightarrow (\mathscr{A} \rightarrow \mathscr{C})$	1, 2 *MP*
	(4)	$\mathscr{B} \rightarrow (\mathscr{A} \rightarrow \mathscr{B})$	(*L*1)
	(5)	$\mathscr{B} \rightarrow (\mathscr{A} \rightarrow \mathscr{C})$	3, 4 *HS*
3(*b*)	(1)	$\mathscr{B} \rightarrow \mathscr{A}$	hipótesis
	(2)	$(\sim \sim \mathscr{B}) \rightarrow \mathscr{B}$	por el Ejercicio 2(*b*) y el Teor de Ded.
	(3)	$(\sim \sim \mathscr{B}) \rightarrow \mathscr{A}$	1, 2 *HS*
	(4)	$\mathscr{A} \rightarrow (\sim \sim \mathscr{A})$	por el Ejercicio 3(*a*)
	(5)	$(\sim \sim \mathscr{B}) \rightarrow (\sim \sim \mathscr{A})$	3, 4 *HS*
	(6)	$((\sim \sim \mathscr{B}) \rightarrow (\sim \sim \mathscr{A})) \rightarrow (\sim \mathscr{A} \rightarrow \sim \mathscr{B})$	(*L*3)
	(7)	$(\sim \mathscr{A}) \rightarrow (\sim \mathscr{B})$	5,6 *MP*
	$\therefore$	$(\mathscr{B} \rightarrow \mathscr{A}) \vdash_{\overline{L}} ((\sim \mathscr{A}) \rightarrow (\sim \mathscr{B}))$	
	luego	$\vdash_{\overline{L}} (\mathscr{B} \rightarrow \mathscr{A}) \rightarrow ((\sim \mathscr{A}) \rightarrow (\sim \mathscr{B}))$	por el Teor de Ded.
3(*d*)	(1)	$\sim (\mathscr{A} \rightarrow \mathscr{B})$	hipótesis
	(2)	$(\mathscr{B} \rightarrow (\mathscr{A} \rightarrow \mathscr{B})) \rightarrow (\sim (\mathscr{A} \rightarrow \mathscr{B}) \rightarrow \sim \mathscr{B})$	por el Ejercicio 3(*b*)
	(3)	$\mathscr{B} \rightarrow (\mathscr{A} \rightarrow \mathscr{B})$	(*L*1)
	(4)	$\sim (\mathscr{A} \rightarrow \mathscr{B}) \rightarrow \sim \mathscr{B}$	2, 3 *MP*
	(5)	$\sim \mathscr{B}$	1,5 *MP*
	(6)	$\sim \mathscr{B} \rightarrow (\mathscr{B} \rightarrow \mathscr{A})$	Proposición 2.11(*a*)
	(7)	$(\mathscr{B} \rightarrow \mathscr{A})$	5, 6 *MP*
	$\therefore$	$\sim (\mathscr{A} \rightarrow \mathscr{B}) \vdash_{\overline{L}} (\mathscr{B} \rightarrow \mathscr{A})$	
	luego	$\vdash_{\overline{L}} (\sim \mathscr{A} \rightarrow \mathscr{B}) \rightarrow (\mathscr{B} \rightarrow \mathscr{A}))$	por el Teor. de Ded.

4 Nótese que el Teorema de Deducción se verifica para L' puesto que ($L3$) no se usa en su demostración.

(i)	(1)	$(\sim\mathscr{A})\rightarrow(\sim\mathscr{B})$	hipótesis
	(2)	$(\sim\mathscr{A})\rightarrow\mathscr{B}$	hipótesis
	(3)	$((\sim\mathscr{A})\rightarrow(\sim\mathscr{B}))\rightarrow(\mathscr{B}\rightarrow\mathscr{A})$	($L3$)
	(4)	$(\mathscr{B}\rightarrow\mathscr{A})$	1, 3 *MP*
	(5)	$(\sim\mathscr{A})\rightarrow\mathscr{A}$	2, 4 *HS*
	(6)	$((\sim\mathscr{A})\rightarrow\mathscr{A})\rightarrow\mathscr{A}$	Proposición 2.11(b)
	(7)	$\mathscr{A}$	5,6 *MP*
(ii)	(1)	$(\sim\mathscr{A})\rightarrow(\sim\mathscr{B})$	hipótesis
	(2)	$\mathscr{B}$	hipótesis
	(3)	$((\sim\mathscr{A})\rightarrow(\sim\mathscr{B}))\rightarrow(((\sim\mathscr{A})\rightarrow\mathscr{B})\rightarrow\mathscr{A})$	($L3$)
	(4)	$((\sim\mathscr{A})\rightarrow\mathscr{B})\rightarrow\mathscr{A}$	1,3 *MP*
	(5)	$B\rightarrow((\sim\mathscr{A})\rightarrow\mathscr{B})$	($L1$)
	(6)	$(\sim\mathscr{A})\rightarrow\mathscr{B}$	2,5 *MP*
	(7)	$\mathscr{A}$	4,6 *MP*

Sección 2.2 (pág. 55)

8 $\mathscr{A}$ no es una tautología, de modo que no es un teorema de L. Aplíquese el Ejercicio 7. L^+ es consistente; en efecto, supóngase lo contrario. Entonces $\vdash_L(\mathscr{A}\rightarrow\mathscr{B})$ y $\vdash_L(\mathscr{A}\rightarrow\sim\mathscr{B})$, para cierta *fbf.* $\mathscr{B}$. Entonces

$$\vdash_L((\sim\mathscr{B})\rightarrow(\sim\mathscr{A}))\text{ y }\vdash_L(\mathscr{B}\rightarrow(\sim\mathscr{A}),$$

y se sigue que $\vdash_L(\sim\mathscr{A})$. Pero $\mathscr{A}$ no es una contradicción, de modo que $(\sim\mathscr{A})$ no es un teorema de L.

10 Sean $\mathscr{A}$ y $\mathscr{B}$ tautologías. Entonces $((\sim\mathscr{A}\rightarrow\mathscr{B})\rightarrow(\mathscr{A}\rightarrow\sim\mathscr{B}))$ es una contradicción, y su negación es un teorema de L, y con ello de L^{++}. Pero se trata de un caso particular del nuevo esquema de axioma, por lo que es el mismo un teorema de L^{++}. Por lo tanto, L^{++} es inconsistente.

12 Usense las Proposiciones 1.10, 2.14 y 2.23.

Capítulo 3

Sección 3.1 (págs. 60-61)

1(a) $\sim(\forall x)(F(x)\rightarrow D(x))$.

(c) $(\exists x)(T(x)\wedge L(x))\rightarrow(\forall x)(T(x)\rightarrow L(x))$.

(f) $(\exists x)(P(x)\wedge(\forall y)(P(y)\rightarrow H(x,\ y)))$.

2(a) $\sim(\forall x)(C(x)\rightarrow T(x))$
$(\exists x)(C(x)\wedge\sim T(x))$.

(c) $(\forall x)(\forall y)((M(x)\wedge E(y))\rightarrow\sim H(x,\ y))$
$\sim(\exists x)(\exists y)(M(x)\wedge E(y)\wedge H(x,\ y))$.

Sección 3.2 (pág. 68)

6 (a), (e), (g), (h).

7 $f_1^2(x_1,\ x_2)$ está libre para x_2 en todas ellas.

8 x_j aparece libre en $\mathscr{A}(x_j)$ sólo si x_i aparecía libre en $\mathscr{A}(x_i)$. Ninguna de estas apariciones puede estar dentro del radio de acción de un $(\forall x_i)$.
9 t está libre para x_1 en (a) y (b).
10 (a) x_2 está libre para x_1 en (b) y (c).
(d) $f_1^3(x_1, x_2, x_3)$ está libre para x_1 solamente en (b).

Sección 3.3 (pág. 71)

11 La interpretación de $\mathscr{A}$ en I es verdadera.
Tómese D_I como $\mathbb{Z}$, $\bar{a}_1$ como 0, $\bar{f}_1^2$ como $+$, $\bar{A}_2^2$ como $=$.
12 Tómese D_I como $\mathbb{Z}$, $\bar{A}_1^1(x)$ como $x>0$, $\bar{f}_1^1(x)$ como $-x$.

Sección 3.4 (págs. 82-83)

14(a) v satisface si $v(x_1)=4$, $v(x_2)=2$, $v(x_3)=6$;
v no satisface si $v(x_1)=1$, $v(x_2)=2$, $v(x_3)=4$.
(b) v satisface si $v(x_1)=1$, $v(x_2)=1$, $v(x_3)=2$;
v no satisface si $v(x_1)=1$, $v(x_2)=1$, $v(x_3)=3$.
15(b) v satisface si $v(x_1)=1$, $v(x_2)=2$;
v no satisface si $v(x_1)=3$, $v(x_2)=2$.
(c) v satisface si $v(x_1)=1$, $v(x_2)=1$;
v no satisface si $v(x_1)=1$, $v(x_2)=2$.
16 (a) falsa; (b), (c), (d) verdaderas.
19(a) Sea I una interpretación y sea v una valoración en I que satisfaga $(\exists x_1)(\forall x_2)\ A_1^2(x_1, x_2)$. Entonces existe v', 1-equivalente a v, que satisface $(\forall x_2)A_1^2(x_1, x_2)$, siendo por ejemplo $v'(x_1)=x$. Entonces toda valoración v'' que sea 2-equivalente a v' satisface $A_1^2(x_1, x_2)$. Supongamos ahora que v no satisface $(\forall x_2)(\exists x_1)A_1^2(x_1, x_2)$. Entonces existe una valoración w, 2-equivalente a v, que no satisface $(\exists x_1)A_1^2(x_1, x_2)$ siendo por ejemplo $w(x_2)=y$. No existe ninguna valoración 1-equivalente a w que satisfaga $A_1^2(x_1, x_2)$. Pero si $v''(x_1)=x$, $v''(x_2)=y$, $v''(x_k)=v(x_k)$ $(k>2)$, entonces v'' es 1-equivalente a w y satisface $A_1^2(x_1, x_2)$.
(c) Sea I una interpretación y sea v una valoración en I que satisfaga

$$(\forall x_1)(\mathscr{A}\rightarrow\mathscr{B}).$$

Entonces, toda v', 1-equivalente a v, satisface $(\mathscr{A}\rightarrow\mathscr{B})$. Supongamos ahora que v no satisface $(\forall x_1)\mathscr{A}\rightarrow(\forall x_1)\mathscr{B}$. Entonces v satisface $(\forall x_1)\mathscr{A}$ y v no satisface $(\forall x_1)\mathscr{B}$, luego existe una v', 1-equivalente a v, que satisface $\mathscr{A}$ y no satisface $\mathscr{B}$. Esta v' no satisface $(\mathscr{A}\rightarrow\mathscr{B})$.
21 Usese la Proposición 3.23.
22(a) Tómese D_I como $\mathbb{Z}$, $\bar{A}_1^2$ como $<$.
(c) Tómese D_I como $\mathbb{Z}$, $\bar{A}_1^2(x)$ como $x=0$, $\bar{a}_1$ como 0.
(d) Esto es falso en N.
23 Proposición 3.23.

Capítulo 4

Sección 4.1 (págs. 91-92)

1 Véase el ejemplo 2.7(a). Usese una vez Generalización.

2(*a*) Demuéstrese primero que $\{\sim\mathscr{B}, (\forall x_i)\mathscr{A}\} \vdash_{\overline{K}} (\forall x_i)\sim(\mathscr{A}\rightarrow\mathscr{B})$. Por el Teorema de Deducción, dedúzcase que

$$\sim\mathscr{B} \vdash_{\overline{K}} ((\forall x_i)\mathscr{A}\rightarrow(\forall x_i)\sim(\mathscr{A}\rightarrow\mathscr{B}))$$

y por tanto que

$$\sim\mathscr{B} \vdash_{\overline{K}} (\sim(\forall x_i)\sim(\mathscr{A}\rightarrow\mathscr{B})\rightarrow\sim(\forall x_i)\mathscr{A})$$

Ahora, por el recíproco del Teorema de Deducción,

$$\{\sim\mathscr{B}, (\exists x_i)(\mathscr{A}\rightarrow\mathscr{B})\} \vdash_{\overline{K}} \sim(\forall x_i)\mathscr{A}$$

y obtenemos $(\exists x_i)(\mathscr{A}\rightarrow\mathscr{B}) \vdash_{\overline{K}} (\sim\mathscr{B}\rightarrow\sim(\forall x_i)\mathscr{A})$, supuesto que x_i no aparezca libre en $\mathscr{B}$. Dos pasos más nos dan el resultado requerido.

(*b*) Análogamente, demuéstrese primero que $\{((\exists x_i)\mathscr{A}\rightarrow\mathscr{B}), \sim\mathscr{B}\} \vdash_{\overline{K}} \sim\mathscr{A}$. Dedúzcase que

$((\exists x_i)\mathscr{A}\rightarrow\mathscr{B}) \vdash_{\overline{K}} (\mathscr{A}\rightarrow\mathscr{B})$, y aplíquese Generalización.

(*c*) Es suficiente demostrar que $\vdash_{\overline{K}} (((\forall x_i)\sim\sim\mathscr{A})\rightarrow(\forall x_i)\mathscr{A})$.

3(*b*) Tómese D_I como $\mathbb{Z}$, $\overline{A}_1^2$ como $<$.

Sección 4.2 (pág. 97)

4 Comienzo: (1) $(\forall x_i)(\mathscr{A}\rightarrow\mathscr{B})$ hipótesis
(2) $(\forall x_i)\mathscr{A}$ hipótesis

5 Es necesario demostrar que

$$\vdash_{\overline{K}} (\sim(\sim(\forall x_i)\sim\mathscr{A})\rightarrow(\forall x_i)(\sim\mathscr{A}))$$

y

$$\vdash_{\overline{K}} ((\forall x_i)(\sim\mathscr{A})\rightarrow(\sim(\forall x_i)\sim\mathscr{A})).$$

6(*a*) Usese ($K5$) dos veces y después Generalización dos veces.
(*b*) Usese ($K5$) en la forma $(\forall x_2)A_1^2(x_1, x_2)\rightarrow A_1^2(x_1, x_1)$.

7 Aplíquese primero la proporción 4.18 a la *fbf.* $\sim\mathscr{A}(x_i)$ obteniendo

$$\vdash_{\overline{K}} (\forall x_i)\sim\mathscr{A}(x_i)\leftrightarrow(\forall x_j)\sim\mathscr{A}(x_j).$$

Sección 4.3 (págs. 102-103)

8(*a*) $(\exists x_3)(\forall x_2)(A_1^1(x_3)\rightarrow A_1^2(x_1, x_2))$.
(*c*) $(\exists x_1)(\forall x_4)(\exists x_3)((A_1^1(x_1)\rightarrow A_1^2(x_1, x_2))\rightarrow(A_1^1(x_4)\rightarrow A_1^2(x_4, x_3)))$.
(Nota: estas respuestas no son únicas).

10 $((\exists x_1)(\exists x_2)A_1^2(x_1, x_2)\rightarrow(\exists x_3))$ es demostrablemente equivalente a *fbfs.* en forma prenex, tanto en forma Π_3 como en forma Σ_3.

Sección 4.4 (pág. 111)

11 Véase la Proposición 2.18. La demostración es en esencia la misma.
12 Supóngase que S no es completo y úsese la Proposición 4.35 dos veces.
13 Tómese $\mathscr{B}$ como $(\sim\mathscr{A})$. $K_{\mathscr{L}}$ no es completo, de modo que podemos tomar $\mathscr{A}$ y $(\sim\mathscr{A})$ de modo que ninguna sea teorema.
14 Ninguna fórmula atómica o negación de fórmula atómica puede ser un teorema de $K_{\mathscr{L}}$. Por la Proposición 4.35, se tiene entonces que el incluir una fórmula atómica o su negación como nuevo axioma dará como resultado una extensión consistente. Diferentes letras de predicado dan lugar a diferentes fórmulas atómicas que proporcionan diferentes extensiones.

Sección 4.5 (pág. 115)

15 Usese inducción sobre el número de pasos de una deducción de $\mathscr{A}$ a partir de Γ. Los axiomas de $K_{\mathscr{L}}$ y los miembros de Γ son todos verdaderos en M, y las reglas de deducción preservan la verdad en M. (Véase la demostración de la Proposición 4.41.) La recíproca no tiene por qué verificarse, salvo que la extensión de $K_{\mathscr{L}}$ obtenida añadiendo como nuevos axiomas todas las *fbfs* de Γ sea completa.
17 S^+ no necesita ser completo. Tómese S como $K_{\mathscr{L}}$, donde $\mathscr{L}$ contiene solamente una letra de predicado A_1^1. M puede construirse de modo que *ninguna* fórmula atómica sea verdadera en M, luego $S^+ = S = K_{\mathscr{L}}$. Ni $(\forall x_1)A_1^1(x_1)$ ni $\sim(\forall x_1)A_1^1(x_1)$ son teoremas de $K_{\mathscr{L}}$.
18 Todos los nuevos axiomas son verdaderos en M, de modo que por el Ejercicio 15, todo teorema de $\hat{S}$ es verdadero en M. Así pues, $\hat{S}$ es consistente. $\hat{S}$ no es necesariamente completo.
19 Véase la demostración de la Proposición 4.46 (considérense los axiomas adicionales $A_1^1(a_i)$, $i \geqslant 1$.

Capítulo 5

Sección 5.2 (pág. 123)

1 Usese la Proposición 3.27 y la validez lógica del axioma ($K5$) para deducir que para toda *fbf* $\mathscr{A}(x_i)$, si $I \models \mathscr{A}(x_i)$ entonces $I \models \mathscr{A}(t)$ para todo término t que esté libre para x_i en $\mathscr{A}(x_i)$. Aplíquese esto a la *fbf*

$$A_1^2(x_1, x_2) \rightarrow A_1^2(f_1^2(x_1, x_2), f_1^2(x_2, x_3))$$

(tres veces, para sustituir términos en lugar de cada una de las variables) y análogamente a $A_1^2(x_1, x_2) \rightarrow A_1^2(f_1^2(x_3, x_2))$.
2 Supóngase lo contrario, y úsense las Proposiciones 4.35 y 5.6.
3 Inducción sobre la longitud de $\mathscr{A}$. El paso base es inmediato a partir de ($E9'$). Paso de inducción: Nótese que si

$$\vdash x_1 = x_2 \rightarrow (\mathscr{B}(x_1) \rightarrow \mathscr{B}(x_2))$$

entonces

$$\vdash x_1 = x_2 \rightarrow (\mathscr{B}(x_2) \rightarrow \mathscr{B}(x_1))$$

ya que

$$\vdash (x_1 = x_2 \rightarrow x_2 = x_1)).$$

y

$$\vdash (x_1 = x_2 \rightarrow x_2 = x_1)).$$

Usese el Teorema de Deducción.

4 A partir de $A_1^2(u_j, v_j)(1 \leqslant j \leqslant n)$ podemos deducir

$$A_i^n(u_1, \ldots, u_n) \leftrightarrow A_i^n(v_1, \ldots, v_n)$$

en S, mediante uso repetido de $(E9)$, suponiendo que u_j y v_j representan variables. Así pues, si $A_1^2(y_j, z_j)$ se verifica en M para cada j,

$$\overline{A}_i^n(y_1, \ldots, y_n)$$

se verifica en M si y sólo si se verifica $A_i^n(z_1, \ldots, z_n)$.

6 Argumentación inductiva similar a la del Ejercicio 3.

Sección 5.3 (págs. 127-128)

7(*a*) Lenguaje: variables, f_1^1, f_1^2, $=$.
Reemplácense (G1)-(G3) por:

$$(\exists x_1)(\forall x_2)(f_1^2(x_1, x_2) = x_2 \wedge f_1^2(f_1^1(x_2), x_2) = x_1).$$

(*b*) Lenguaje: variables, a_1, $=$, A_1^3.
$(A_1^3(x_1, x_2, x_3)$ a interpretar como $x_1 x_2 = x_3)$
Reemplácense $(G1)$-$(G3)$ por:

$$(\forall x_1)(\forall x_2)(\exists_1 x_3) A_1^3(x_1, x_2, x_3),$$

$$(A_1^3(x_1, x_2, x_4) \wedge A_1^3(x_4, x_3, x_5) \wedge A_1^3(x_2, x_3, x_6)$$

$$\wedge A_1^3(x_1, x_6, x_7)) \Rightarrow x_5 = x_7,$$

$$(\forall x_2)(\exists x_1) A_1^3(x_1, x_2, a_1)$$

y

$$(\forall x_1) A_1^3(a_1, x_1, x_1).$$

9 El incluir a_1 produce el efecto de distinguir un elemento del modelo, a saber $\bar{a}_1$, y no tiene ninguna significación en cuanto a cuál es el elemento escogido. Análogamente ocurre con una sucesión $a_1, a_2, \ldots$, y las interpretaciones de estos símbolos no es necesario que sean todas elementos diferentes.

12 Denótese por kx_1 la suma de x_1 consigo mismo k veces $(k > 1)$ en $\mathscr{F}$, y por (Ck) la *fbf.* $(kx_1 = 0) \Rightarrow (x_1 = 0)$ de $\mathscr{F}$. Cada (Ck) es verdadera en cuerpos de característica 0; de hecho, $\mathscr{F}$ con estos axiomas adicionales da un sistema de la teoría de cuerpos de característica cero. Ahora bien, si $\mathscr{A}$ es verdadera en todo modelo de este sistema, es un teorema del sistema. En una demostración de $\mathscr{A}$ solamente se usa un número finito de axiomas, de modo que podemos suponer que no se usa ninguna (Ck) con $k > n$. Los cuerpos de característica p con $p > n$ son modelos de $\mathscr{F}$ con los axiomas

adicionales $(C2), \ldots, (Cn)$. $\mathscr{A}$ es un teorema de este sistema, luego es verdadera en todo modelo de este tipo.

13 Usénse las ideas del Ejercicio 12, y véase el Corolario 4.47.

Sección 5.4 (pág. 132)

14 Los axiomas para $\mathscr{N}'$ no mencionan específicamente a_0, de modo que su interpretación no está constreñida a tener ninguna propiedad particular. Si se escoge $\bar{a}_0$ como r, entonces la *fbf* $\sim(a_0 = a_i)$ es verdadera en $\mathscr{N}'$ para todo $i \leqslant r$. Así, pues, para cada r el conjunto de *fbfs* $\{\sim(a_0 = a_i) : 0 < i \leqslant \leqslant r\}$ tiene un modelo, y el sistema obtenido a partir de $\mathscr{N}'$ incluyéndolas como axiomas es consistente. Por lo tanto, el sistema obtenido incluyendo todas estas *fbfs* para $i > 0$ es consistente (por una argumentación familiar —véase, por ejemplo, la demostración de la Proposición 2.21). Un modelo así se llama modelo no-standard de la aritmética, porque incluye todos los números naturales y al menos otro elemento. Naturalmente este otro elemento debe tener sucesores y predecesores, sumas y productos con números naturales y consigo mismo, etc.

Sección 5.5 (pág. 137)

15 Reemplácese $(ZF2)$ por: $(\forall x_1)\sim(x_1 \in a_1)$.
Añádase $(ZF2')$: $A_3^2(t_1, t_2) \leftrightarrow (\forall x_1)(x_1 \in t_1 \rightarrow x_1 \in t_2)$.
Reemplácese $(ZF3)$ por: $(\forall x_1)(\forall x_2)(\forall x_3)(x_3 \in f_1^2(x_1, x_2) \leftrightarrow x_3 = x_1 \vee x_3 = x_2)$.
Los elementos del dominio D de esta interpretación son 0, 1, 2, ..., siendo $0 = \varnothing$ y $n = \{0, 1, \ldots, n-1\}$ para $n \neq 0$. Para $(ZF1)$: si $m = n = 0$ entonces ni m ni n tienen miembros; si $m = n \neq 0$ entonces ambos tienen 0, 1, ..., $m-1$ como miembros, y recíprocamente, si m y n tienen los mismos miembros, entonces o son ambos 0 o $\{0, 1, \ldots, m-1\} = \{0, 1, \ldots, n-1\}$, luego $m = n$. Para $(ZF2)$: Está claro que 0 es el conjunto vacío. Para $(ZF3)$: Considérense 2, $3 \in D$. $\{2, 3\} \notin D$, luego $(ZF3)$ es falso. Para $(ZF4)$: $\bigcup 0 = 0$, $\bigcup 1 = 0$ y $\bigcup\{0, 1, \ldots, m-1\} = \{0, 1, \ldots, m-2\} = m-1 \in D$. Para $(ZF5)$: los subconjuntos del conjunto 2 son $\varnothing, \{0\}, \{1\}$ y $\{0,1\}$, y estos elementos no constituyen un miembro de D. Para $(ZF7)$: supóngase que m es el conjunto cuya existencia afirma $(ZF7)$ —entonces $m \neq 0$, ya que $0 \notin 0$ si $m = \{0,1, \ldots, m-1\}$ entonces $m - 1 \in m$ y $(m-1) \cup \{m-1\} \notin m$, porque $m \notin m$. Para $ZF8$), si $m = \{0, 1, \ldots, m-1\}$, entonces $0 \in m$. y 0 no tiene elementos en común con m.

$(ZF6)$ es falso. Tómese $\mathscr{A}(x_1, x_2)$ como $x_2 = \{x_1\}$. Entonces la imagen del conjunto 2 (por ejemplo) no es miembro de D.

Capítulo 6

Sección 6.2 (págs. 148-149)

1 Por el Ejemplo 6.7, si $m + r = n$ entonces $\vdash_{\mathscr{N}} 0^{(m)} + 0^{(r)} = 0^{(n)}$.
Usando el axioma $(K5)$ en la forma

$$(\forall x_1)\sim(0^{(m)} + x_1 = 0^{(n)}) \rightarrow \sim(0^{(m)} + 0^{(r)} = 0^{(n)})$$

podemos deducir $\vdash_{\mathscr{N}} \sim(\forall x_1)\sim(0^{(m)}+x_1=0^{(n)})$ como se requería.

2 Sea $m>n$. Entonces $m=n+r$ con $r>0$. Por tanto, $\vdash_{\mathscr{N}} 0^{(m)}+0^{(n)}+0^{(r)}$ y $\vdash_{\mathscr{N}} 0^{(m)}+x_1=0^{(n)}+0^{(r)}+x_1$. Ahora bien, $\vdash_{\mathscr{N}} 0^{(n)}+0^{(r)}+x_1=0^{(n)}$ implica $\vdash_{\mathscr{N}} 0^{(r)}+x_1=0$ (véase la demostración de la Proposición 6.1) y

$$\vdash_{\mathscr{N}} 0^{(r)} + x_1 = (0^{(r-1)} + x_1)'$$

por $(N4^*)$, ya que $r > 0$. Así pues,

$$\vdash_{\mathscr{N}} 0^{(n)}+0^{(r)}+x_1=0^{(n)}\rightarrow \sim(N1^*),$$

y con ello

$$\vdash_{\mathscr{N}} \sim(0^{(n)}+0^{(r)}+x_1=0^{(n)}, \text{ es decir } \vdash_{\mathscr{N}}\sim(0^{(m)}+x_1=0^{(n)}).$$

Por Generalización, $\vdash_{\mathscr{N}} (\forall x_1)\sim(0^{(m)}+x_1=0^{(n)})$ de donde se deduce el resultado.

3 (*a*) $\sim(\forall x_1)(\forall x_2)\sim(x_1x_2=0^{(n)})$.

(*c*) Reescríbase $m=\min(p,q)$ como: $(p\leqslant q \wedge m=p) \vee (q<p \wedge m=q)$.

(*e*) Reescríbase en la forma $(m=0 \wedge n=0) \vee (m\neq 0 \wedge n=1)$.

4 (*a*) Para $m=0$, $n=0$, demuéstrese que
$\vdash_{\mathscr{N}} (0^{(0)}=0 \wedge 0^{(0)}=0) \vee (0^{(0)}\neq 0 \wedge 0^{(0)}=0^{(1)})$.

Para $m\neq 0$, $n=1$, demuéstrese que

$$\vdash_{\mathscr{N}} (0^{(m)}=0 \wedge 0^{(1)}=0) \vee (0^{(m)}\neq 0 \wedge 0^{(1)}=0^{(1)}).$$

Para $m=0$, $n\neq 0$, demuéstrese que

$$\vdash_{\mathscr{N}} \sim(0^{(0)}=0 \wedge 0^{(n)}=0) \vee (0^{(o)}\neq 0 \wedge 0^{(n)}=0^{(1)}).$$

Para $m \neq 0$, $n = 0$, demuéstrese que

$$\vdash_{\mathscr{N}} \sim((0^{(m)}=0 \wedge 0^{(o)}=0) \vee (0^{(m)}\neq 0 \wedge 0^{(o)}=0^{(1)}).$$

Finalmente, para $m=0$ y $m\neq 0$ separadamente

$$\vdash_{\mathscr{N}} (\exists_1(x_1)((0^{(m)}=0 \wedge x_1=0) \vee (0^{(m)}\neq 0 \wedge x_1=0^{(1)})).$$

(*b*) Sea $\mathscr{A}(x_1,x_2)$ la *fbf.* $x_2=x_1+0^{(3)}$.

Si $n=m+3$, entonces $\vdash_{\mathscr{N}} 0^{(n)}=0^{(n)}+0^{(3)}$.

Si $n\neq m+3$, entonces $\vdash_{\mathscr{N}}\sim(0^{(n)}=0^{(m)}+0^{(3)})$.

Así pues, para todo $m \in D_N$, $\vdash_{\mathscr{N}}(\exists_1 x_2)(x_2=0^{(m)}+0^{(3)})$.

(Alternativamente, úsese el Ejemplo 6.7).

(*c*) Tómese como $(\mathscr{A}(x_1,x_2)$ la *fbf.*

$$(\exists x_3)((x_1 = x_2 + x_3 \times 0^{(2)}) \wedge (x_2 = 0 \vee x_2 = 1))$$

5 Este es un ejercicio complicado de uso del Teorema de Deducción. Hemos de demostrar que si $f(m)\neq n$ entonces $\vdash_{\mathscr{N}} \sim\mathscr{A}(0^{(m)}, 0^{(n)})$. Sea $f(m)=p$. Necesitamos demostrar:

$$\{0^{(n)}\neq 0^{(p)},\mathscr{A}(0^{(m)},0^{(p)}),(\exists_1 x_2)\mathscr{A}(0^{(m)},x_2)\} \vdash_{\mathscr{N}} \sim\mathscr{A}(0^{(m)},0^{(n)}).$$

Es suficiente demostrar:

$$\{0^{(n)} \neq 0^{(p)}, \mathscr{A}(0^{(m)}, 0^{(p)})\} \vdash_{\mathscr{N}} (\exists_1 x_2).\mathscr{A}(0^{(m)}, x_2) \rightarrow \sim \mathscr{A}(0^{(m)}, 0^{(n)})$$

o

$$\{0^{(n)} \neq 0^{(p)}, \mathscr{A}(0^{(m)}, 0^{(p)})\} \vdash_{\mathscr{N}} \mathscr{A}(0^{(m)}, 0^{(n)}) \rightarrow \sim (\exists_1 x_2).\mathscr{A}(0^{(m)}, x_2)$$

o

$$\{0^{(n)} \neq 0^{(p)}, \mathscr{A}(0^{(m)}, 0^{(p)}), \mathscr{A}(0^{(m)}, 0^{(n)})\} \vdash_{\mathscr{N}} \sim (\exists_1 x_2).\mathscr{A}(0^{(m)}, x_2).$$

Intuitivamente, esto está claro, pero aún quedan dificultades técnicas. Necesitamos

$$\{0^{(n)} \neq 0^{(p)}, \mathscr{A}(0^{(m)}, 0^{(p)}), \mathscr{A}(0^{(m)}, 0^{(n)})\} \vdash_{\mathscr{N}}$$
$$(\forall x_2) \sim (\mathscr{A}(0^{(m)}, x_2) \wedge (\forall x_3)(\mathscr{A}(0^{(m)}, x_3) \rightarrow x_3 = x_2)).$$

Esta última *fbf.* es equivalente a

$$(\forall x_2)(\mathscr{A}(0^{(m)}, x_2) \rightarrow \sim (\forall x_3)(\mathscr{A}(0^{(m)}, x_3) \rightarrow x_3 = x_2)).$$

De modo que demostramos que

$$\{0^{(n)} \neq 0^{(p)}, \mathscr{A}(0^{(m)}, 0^{(p)}), \mathscr{A}(0^{(m)}, 0^{(n)}), \mathscr{A}(0^{(m)}, x_2)\}$$
$$\vdash_{\mathscr{N}} \sim (\forall x_3 (\mathscr{A}(0^{(m)}, x_3) \rightarrow x_3 = x_2)$$

demostrando que

$$\{\mathscr{A}(0^{(m)}, 0^{(p)}), \mathscr{A}(0^{(m)}, 0^{(n)}), \mathscr{A}(0^{(m)}, x_2), (\forall x_3)(\mathscr{A}(0^{(m)}, x_3)$$
$$\rightarrow x_3 = x_2)\} \vdash_{\mathscr{N}} 0^{(n)} = 0^{(p)}.$$

(Nota: Podemos no usar Generalización sobre x_2 en este último paso.)

6 Tómese $\mathscr{A}(x_1, \ldots, x_{k+1})$ como $x_{k+1} = x_i$.

Sección 6.3 (págs. 157-158)

7(*a*) $e(m, 0) = 1$

$e(m, n+1) = m \times e(m, n)$.

Ahora bien, $e(m,0)$ es una función constante de m, y ésta es recursiva primitiva. Por lo tanto, $m \times e(m,n)$ es una función recursiva primitiva de m,n y $e(m,n)$.

Podemos escribir $m \times e(m, n)$ como $h(m, n, e(m, n))$, siendo $h(m, n, p)$. $= p_1^3(m,n,p) x p_3^3(m,n,p)$. La dependencia de n no es explícita en $m \times e(m,n)$ y a causa del procedimiento empleado más arriba, no necesita serlo.

(*b*) $\min(m, n) = m \dot{-} (m \dot{-} n)$.

(*c*) Defínase primero $rm(m,n) =$ resto de la división de n entre m si $m \neq 0$; 0 si $m = 0$.

Entonces $rm(m,0) = 0$

$$rm(m,n+1) = sg(m) \times sg((m \dot{-} 1) \dot{-} rm(m,n)) \times (1 + rm(m, n)),$$

de modo que rm es recursiva primitiva, ya que $+, \times, \dot{-}$, y sg lo son. Ahora $q(m,0) = 0$

$$q(m,n+1) = sg(m) \times (q(m,n) + \bar{sg}((m \dot{-} 1) \dot{-} rm(m,n)),$$

luego q es recursiva primitiva, ya que $+, \times, \dot{-}, sg, \bar{sg}$ y rm lo son.

8 R es recursiva, de modo que C_R es recursiva, y $R(n_1, \ldots, n_k, x)$ se verifica si y sólo si $C_R(n_1, \ldots, n_k, x) = 0$.

9 $e_2(n) = \mu x[\bar{sg}(rm(2^x, n)) = 0] \dot{-} 1$.

11 Sea $k(n_1, n_2) = n_1^{n_2}$. k es recursiva, f y g son recursivas; luego h es recursiva por composición, pues

$$h(x) = k(f(x), g(x)).$$

14 Defínanse relaciones de un argumento $R_1, R_2, \ldots$, poniendo:

$R_i(n)$ se verifica si y sólo si $R(i,n)$ se verifica.

Entonces, $S(n)$ se verifica si y sólo si $R_1 \vee R_2 \vee \ldots \vee R_{k-1}$ se verifica, y

$T(n)$ se verifica si y sólo si $R_1 \wedge R_2 \wedge \ldots \wedge R_{k-1}$ se verifica.

Si se elimina la condición '$< k$', estas relaciones ya no son necesariamente recursivas. Considérese un conjunto no recursivo X, enumerado como $\{x_1, x_2, \ldots\}$ y sea $X_i = \{x_1, \ldots, x_i\}$, para $i \geqslant 1$. Entonces, $R(m, n)$ se verifica si y sólo si $n \in X_m$. Los R_i definidos como más arriba son recursivas, ya que los X_i son conjuntos finitos, pero $S^\infty(n)$ no es recursiva, supuesto que $S^\infty(n)$ se verifica si y sólo si existe un m tal que $R(m,n)$. En efecto, $S^\infty(n)$ se verifica si y sólo si $n \in X$, y X no es recursivo.

Sección 6.4 (pág. 163)

15(*a*) $65 = 9 + 8 \times 7 = g(a_7)$.

(*b*) $299 = 11 + 8 \times 36 = 11 + 8 \times (2^2 \times 3^2) = g(f_2^2)$.

(*c*) $109 = 13 + 8 \times 12 = 13 + 8 \times (2^2 \times 3) = g(A_1^2)$.

(*d*) $421 = 13 + 8 \times 51 \neq g(t)$ para todo símbolo t.

16(*a*) $A_1^1(x_1)$.

(*b*) $\sim A_1^1(x_1)$.

(*c*) $(\forall x_1) A_1^1(x_1)$.

17 Si $s = a_1, a_2, \ldots, a_u$ y $t = b_1, \ldots, b_v$ entonces

$$m = p_1^{a_1} \times \ldots \times p_u^{a_u} \text{ y } n = p_1^{b_1} \times \ldots \times p_v^{b_v}.$$

Ahora bien

$$s * t = a_1, a_2, \ldots, a_u, b_1, \ldots, b_v,$$

luego

$$f(m, n) = p_1^{a_1} \times \ldots \times p_u^{a_u} \times p_{u+1}^{b_1} \times \ldots \times p_{u+v}^{b_v}.$$

Pero $b_i = e_i(n)$, $u = \mu x[\bar{sg}(rm(p_x, m)) = 0] - 1$ y como p_x es función recursiva de x (véase el Ejemplo 6.25 (*a*)) u es función recursiva de m. Análogamente, v es función recursiva de n, luego

$$f(m, n) = m \times p_{u+1}^{e_1(n)} \times \cdots \times p_{u+v}^{e_v(n)} \text{ es recursiva.}$$

Sección 6.5 (pág. 168)

18 Denótese la extensión por $\mathscr{N}^+$. Entonces $\vdash_{\overline{\mathscr{N}^+}} \sim\mathscr{U}$,

es decir, $\vdash_{\overline{\mathscr{N}^+}} \sim(\forall x_2)\sim\mathscr{W}(0^{(p)},x_2)$.

Pero en la demostración de la Proposición 6.32 se demuestra que $\vdash_{\overline{\mathscr{N}}} \sim\mathscr{W}(0^{(p)}, 0^{(q)})$ para todo q. Por tanto, $\vdash_{\overline{\mathscr{N}}} \sim\mathscr{W}(0^{(p)}, 0^{(q)})$ para todo q, y $\mathscr{N}^+$ no es ω – consistente.

Capítulo 7

Sección 7.1 (pág. 177)

1(*a*) En el Capítulo 6 hemos descrito métodos para encontrar qué símbolos o cadenas de símbolos corresponden a números de Gödel dados. Dado n, encuéntrese qué símbolos (si los hay) corresponden a él. Si es una variable o una constante, dese la respuesta «sí». Si es otro símbolo, respóndase «no». Si no hay ningún símbolo, encuéntrese qué cadena de símbolos corresponde. Si es un término, contéstese «sí». Si es otra cadena, o si no hay ninguna cadena, contéstese «no».

(*c*) Calcúlense los cuadrados de todos los enteros positivos hasta encontrar $x^2 \geqslant n$. Si n no ha aparecido en la lista en este momento, entonces no es un cuadrado perfecto.

(*d*) Constrúyanse tablas de verdad para todas las *fbfs*, *de* Γ y para Γ. $\Gamma \vdash \mathscr{A}$ si y sólo si $\mathscr{A}$ es V siempre que todas las *fbfs*. de Γ sean V.

(*f*) Hágase una lista de todos los primos, comprobando por turno para cada entero positivo si es primo o no, y poniendo en la lista solamente los primos.

2 Sean A y $\bar{A}$ recursivamente enumerables. Sean entonces $f(0), f(1), f(2), \ldots$ y $g(0), g(1), g(2), \ldots$ enumeraciones efectivas de A y $\bar{A}$. Sea $n \in D_N$. Escríbanse (simultáneamente) las listas de más arriba, correspondientes a A y $\bar{A}$. n tiene que aparecer en una de las listas. Cuando aparezca, la lista en la que está nos dice si $n \in A$ o $n \in \bar{A}$. Existe un conjunto X que no es recursivo. Entonces $\bar{X}$ es no recursivo (Corolario 6.23). Uno al menos de entre X y $\bar{X}$ ha de ser no recursivamente enumerable, ya que si ambos lo fueran serían recursivos.

3 Dado x, enumérese A hasta encontrar el primer elemento $\geqslant x$. $x \in A$ si y sólo si x está en la lista.

4(*a*) Usese la Tesis de Church. Dado n, para cada $p<n$ encuéntrese si p y n tienen factores comunes. Cuéntense aquellos p que los tienen. Esto es un algoritmo para calcular φ.

(*c*) O bien hay sucesiones de 7s de longitud arbitraria, o hay una cota superior, digamos que k, de las longitudes de estas sucesiones. En el primer caso $g(n)=0$ para todo $n \in D_N$ (con lo que g es recursiva). En el segundo caso

$$g(n)=\begin{cases}0 & \text{para } 0\leqslant n\leqslant k\\ 1 & \text{para } n>k\end{cases}$$

y esta función es recursiva también.

5(*a*) D_N.

(*b*) El conjunto de números de Gödel de teoremas de $\mathcal{N}$. El conjunto de los números de Gödel de las *fbfs.* de $\mathcal{N}$ que son tautologías es un subconjunto recursivo.

6 Véase el Ejercicio 3. Dada una enumeración efectiva del conjunto A, escójase una enumeración *creciente* de un subconjunto B. B será recursivo.

Sección 7.2 (págs. 197-198)

7 La cinta inicial necesitará una marca, digamos M, en el extremo derecho de la parte no blanca. Añádanse las cuádruplas $(q_0\ \mathrm{B}\ D\ q_0)$ y $(q_0\ \mathrm{M}\ \mathrm{D}\ q_2)$.

9 $\{(q_0\,\mathrm{B}\,D\,q_0),(q_0,\ 1,\ D,\ q_0)\}$
ó
$\{(q_0\ \mathrm{B}\ D\ q_1),\ (q_0\ 1\ D\ q_1),\ (q_1\ \mathrm{B}\ I\ q_0),\ (q_1\ 1\ I\ q_0)\}$,

10 $\{(q_0\,1\,\mathrm{A}\,q_1),(q_1\,\mathrm{A}\,D\,q_2),(q_2\,1\,D\,q_2),(q_2\,\mathrm{B}\,\mathrm{X}\,q_2),$
$(q_2\,\mathrm{X}\,D\,q_3),(q_3\,\mathrm{B}\,I\,q_4),(q_3\,1\,D\,q_3),(q_4\,1\,I\,q_4),$
$(q_4\,\mathrm{X}\,I\,q_4),(q_4\,\mathrm{A}\,D\,q_0),(q_0\,\mathrm{X}\,I\,q_5),(q_5\,\mathrm{A}\,I\,q_5),(q_5\,1\,I\,q_5)\}$
La máquina comienza en estado q_0 leyendo el 1 de más a la izquierda.

11 Véase el Ejemplo 7.13 $\{(q_0,\ 1,\ D,\ q_1),\ (q_1,\ 1,\ q_0),\ (q_0\ \mathrm{B}\ D\ q_0)\}$ (si el número de entrada es par, la cuádrupla $(q_0\ \mathrm{B}\ D\ q_0)$ asegura que la máquina nunca para para obtener T', omítase $(q_0\ \mathrm{B}\ D\ q_0)$, *y añádanse los cuádruplos* $(q_0\ \mathrm{B}\ I\ q_2)$, $(q_0\ 1\ \mathrm{B}\ q_3)$, $(q_3\ \mathrm{B}\ I\ q_2)$. Considérese la lista φ^0, φ_1, ..., de todas las funciones parciales recursivas. Entonces, $f(n)=\varphi_n(n)+1$ es una función *parcial* recursiva que no puede extenderse a una función *total* recursiva. En efecto, supongamos que φ_k es total y que $\varphi_k(n)=\varphi_n+1$ siempre que $\varphi_n(n)$ exista. Ahora, φ_k es total, luego $\varphi_k(k)$ existe, y $\varphi_k(k)=\varphi_k(k)+1$. Contradicción. (Véase el Ejemplo que precede a la Proposición 7.28.)

12 Supongamos que el alfabeto de símbolos para la cinta contiene n símbolos, y que hay k estados internos. Si la máquina no se mueve de un cuadro dado en $nk+1$ pasos, no parará nunca, ya que en ese tiempo debe repetir un par (estado, símbolo leído) y partir de ahí seguirá repitiendo para siempre una acción periódica. (Por supuesto, puede parar antes de $nk+1$ pasos.) Si la parte no blanca de la cinta constaba originalmente de p cuadros, entonces después de $p(nk+1)$ pasos podemos estar seguros de que la máquina habrá parado, o se habrá salido del extremo derecho de la parte no blanca de la cinta, o habrá entrado en un bucle «estacionario» como se ha descrito arriba. Si se sale del extremo derecho de la parte no blanca de la cinta, entonces puede moverse a lo sumo k cuadros más a la derecha sin repetir una combinación (estado, blanco). Así pues, si se mueve $k+1$ cuadros más, entrará forzosamente en un patrón repetitivo. Ahora bien, después de $(k+1)(nk+1)$ pasos más, habrá parado, o entrado en un bucle estacionario, o se habrá movido $k+1$ cuadros a la derecha. Podemos pues decir de antemano que si la máquina va a parar lo hará en $(p+k+1)\,(nk+1)$ pasos o menos, de modo que el algoritmo consiste en hacer funcionar la máquina hasta que pare o llegue a dar $(p+k+1)(nk+1)$ pasos.

15 Supongamos que $n \in K$. Entonces T_n para con entrada n, luego $n \in A$. Pero $A \leqslant \bar{K}$, luego $n \in \bar{K}$. Contradicción, luego $n \in \bar{K}$. Supongamos ahora que $n \in A$. Entonces T_n para con entrada n, luego $n \in K$. Contradicción, luego $n \notin A$. Por tanto, $n \in \bar{K} \setminus A$.

16 Sea X recursivamente enumerable. Supongamos que X es enumerable por la función recuersiva f. Definamos g poniendo

$$g(y) = \mu x[f(x) = y]$$

Como f es recursiva, g es una función parcial recursiva, y su dominio es X. Por la Proposición 7.25, g es Turing-computable, y por lo tanto existe una máquina de Turing de dominio X.

17(*e*) {¿para T_n para todo número de entrada/$n \in D_N$} Consideremos el siguiente algoritmo: Sea m fijo, Dado n, sígase el cómputo de T_m, con entrada m; y si para, dese salida n. Este algoritmo puede transformarse primero en intrucciones para una máquina de Turing y segundo en un número de código $k(m)$ para una máquina de Turing $T_{k(m)}$. $T_{k(m)}$ tiene la propiedad de que si T_m para con entrada m, entonces $T_{k(m)}$ para cualquier entrada, y si T_m no para con entrada m, entonces $T_{k(m)}$ no para con ninguna entrada. Para decidir ahora si T_m para con entrada m sólo necesitamos calcular $k(m)$ y responder a la pregunta: ¿para $T_{k(m)}$ para toda entrada? Por lo tanto, la solubilidad de la clase de problemas propuesta implicaría que K es recursivo.

(*f*) {¿Para T_n para algún número de entrada?/$n \in D_N$}. $T_{k(m)}$ (en (*e*) más arriba) o bien no para con ninguna entrada o para con cualquier entrada dependiendo de m. Por lo tanto, si pudiésemos decidir si $T_{k(m)}$ para con algún número de entrada, podríamos decidir la pertenencia a K, como en (*e*).

18 Un algoritmo para decidir la pertenencia a K_0 proporcionaría claramente un algoritmo para decidir la pertenencia a K, de modo que K es reducible a K_0. Supongamos ahora que existiese un algoritmo para K. Consideremos el algoritmo: Sean m,n fijos. Dado p, sígase el cómputo de T_m con entrada n; y si éste se obtiene, dese salida p. Igual que en el Ejercicio 17(*e*), este algoritmo proporciona instrucciones para una máquina de Turing y con ello un número de código $k(m,n)$ para esta máquina, y $T_{k(m,n)}$ para con toda entrada p o con ninguna entrada, dependiendo de si T_m para con entrada n. Así pues, para decidir si $(m,n) \in K_0$ sólo necesitamos calcular $k(m, n)$ y responder a la pregunta: ¿Para $T_{k(m,\ n)}$ con entrada $k(m, n)$? Es decir, ¿se tiene $k(m, n) \in K$?

Sección 7.3 (pág. 204)

19 (*a*) Puede demostrarse fácilmente que cualquier palabra dada es equivalente a una palabra que esté en una de las formas standard:

$$a_1 a_2^{k_1} a_1 a_2^{k_2} a_1 \cdots a_1 a_1^{k_n} a_1 \qquad (n \geqslant 1),$$

$$a_1^{k_1} a_1 a_2^{k_2} a_1 \cdots a_1 a_2^{k_n} a_1 \qquad (n \geqslant 0),$$

$$a_2^{k_1} a_1 a_2^{k_2} a_1 \cdots a_1 a_2^{k_n} \qquad (n \geqslant 1).$$

Dos palabras en forma standard son equivalentes si y sólo si son idénticas, de modo que dos palabras dadas son equivalentes si se reducen como más arriba a la *misma* forma standard.

(*b*) Nótese que $a_3a_2 \sim a_1a_2a_2 \sim a_1a_2 \sim a_3$.
Puede demostrarse que cualquier palabra dada es equivalente a una que está en la forma

$$a_1^{k_1}a_3^{k_2}a_1^{k_3} \cdots a_1^{k_{n-1}}a_3^{k_n},$$

donde todas las apariciones de a_1 se han «absorbido».

20 G es un grupo abeliano. El ver que los símbolos $a_1^{-1}, a_2^{-1}, a_3^{-1}$ conmutan entre sí y con los otros símbolos es un ejercicio de manipulación. Por ejemplo:

$$e \sim a_2^{-1}a_1^{-1}a_1a_2 \Rightarrow e \sim a_2^{-1}a_1^{-1}a_2a_1$$
$$\Rightarrow ea_1^{-1} \sim a_2^{-1}a_1^{-1}a_2a_1a_1^{-1} \sim a_2^{-1}a_1^{-1}a_2 \Rightarrow a_1^{-1}a_2^{-1} \sim a_2^{-1}a_1^{-1}$$

y

$$a_1a_2^{-1}a_1^{-1}a_2 \sim a_1a_1^{-1}a_2^{-1}a_2 \sim e,$$

y luego

$$a_1a_2^{-1}a_1^{-1}a_2a_2^{-1} \sim a_2^{-1}$$

y

$$a_1a_2^{-1}a_1^{-1}a_1 \sim a_2^{-1}a_1,$$

es decir,

$$a_1a_2^{-1} \sim a_2^{-1}a_1.$$

Cualquier palabra dada puede reducirse a una forma standard $a_1^{r_1}a_2^{r_2}a_3^{r_3}$, siendo $r_1, r_2, r_3, \in \mathbb{Z}$. Dos palabras dadas son equivalentes si y sólo si sus formas standard son idénticas.

22 Al igual que una máquina de Turing puede reemplazarse por otra equivalente que use exactamente dos símbolos de cinta (Observación 7.22), podemos construir esencialmente el mismo semigrupo $\mathscr{S}$ del Teorema 7.37 usando sólo dos símbolos. Los símbolos de $\mathscr{S}$ pueden codificarse en forma monaria, con un 0 al comienzo para servir de marca. Por ejemplo, q_0 sería 01, q_4 sería 011111 y la palabra $q_0q_4q_1$ sería 01011111011.

Sección 7.4 *(págs. 212-213)*

24(*a*) $\{n \in D_N : n$ es el número de Gödel de $\sim\mathscr{A}$, siendo $\mathscr{A}$ un teorema de $\mathscr{N}\}$ no es recursivo. Dado $n \in D_N$, decídase si es el número de Gödel de una *fbf* $\mathscr{A}$ de $\mathscr{N}$. Si lo es, calcúlese el número de Gödel de $(\sim\mathscr{A})$ (esto puede hacerse de modo efectivo —véase la Sección 6.4). Si el conjunto dado fuese recursivo, entonces el conjunto de números de Gödel de teoremas de $\mathscr{N}$ sería recursivo.

(*b*) $\{n \in D_N : n$ es el número de Gödel de $\mathscr{A}$, siendo $\mathscr{A}$ verdadera en $N\}$ no es recursivo (Capítulo 6). $\mathscr{A}$ es verdadera en N si y sólo si $(\sim\mathscr{A})$ es falsa. Por lo tanto, la recursividad del conjunto dado llevaría a una contradicción.

26 Si $\mathscr{V}$ es verdadera en N, entonces $F(p,s)$ se verifica para algún $s \in D_N$, y por tanto $f(s)$ es el número de Gödel de $(\exists x_2)\mathscr{F}(0^{(p)},x_2)$ para algún s, con lo que $\mathscr{V}$ es falsa en N. $\mathscr{V}$ es cerrada, luego debe ser falsa en N. Si $q=f(k)$ (siendo q el número de Gödel de $\mathscr{V}$) entonces $f(k)$ es el número de Gödel de $(\exists x_2)\mathscr{F}(0^{(p)}, x_2)$, con lo que se verifica $F(p, k)$. Por lo tanto, $\vdash_{\mathscr{N}} \mathscr{F}(0^{(p)}, 0^{(k)})$, y así $\vdash_{\mathscr{N}} (\exists x_2)\mathscr{F}(0^{(p)}, x_2)$, es decir, $\vdash_{\mathscr{N}} \mathscr{V}$, con lo que $\mathscr{V}$ es verdadera en N. Contradicción, luego q no está en el rango de f.

27 Si el conjunto de los (números de Gödel de los) axiomas de T es recursivo, entonces el conjunto de los (números de Gödel de los) teoremas de T es recursivamente enumerable (Observación 7.6). Los sistemas S y T tienen el mismo conjunto de teoremas. Si S es completo y el conjunto de (los números de Gödel de) sus teoremas es recursivamente enumerable, entonces dado cualquier $n \in D_N$, si es número de Gödel de una *fbf* $\mathscr{A}$ de S, enumérense todos los (números de Gödel de) teoremas de S. $0\mathscr{A}$ o $\sim\mathscr{A}$ es un teorema de S, y en su momento encontraremos cuál. Luego S es recursivamente decidible.

Bibliografía

COHEN, P. J, *Set Theory and the Continuum Hypothesis*, Addison-Wesley, 1966.

COPI, I. M, *Introduction to Logic*, Macmillan, 1961.

DAVIS, M (1), Hilbert's tenth problem is unsolvable, *American Mathematical Monthly*, Vol. 80 (1973) p. 233.

DAVIS, M (2), *Computability and Unsolvability*, McGraw-Hill, 1958.

HALMOS, P. R, *Naive Set Theory*, Van Nostrand, 1960.

HILBERT, D, Mathematical problems, *Bulletin of the American Mathematical Society*, Vol 8 (1901–2) p. 437.

KLEENE, S. C, *Introduction to Metamathematics*, Van Nostrand, 1952.

MENDELSON, E, *Introduction to Mathematical Logic*, Van Nostrand, 1964.

MINSKY, M, *Computation: Finite and Infinite Machines*, Prentice-Hall, 1967.

ROBINSON, A, *Introduction to Model Theory and to the Metamathematics of Algebra*, North-Holland, 1965.

ROGERS, H, *Introduction to the Theory of Recursive Functions and Effective Computability*, McGraw-Hill, 1967.

SHOENFIELD, J. R, *Mathematical Logic*, Addison-Wesley, 1967.

TARSKI, A, MOSTOWSKI, A, AND ROBINSON, R. M, *Undecidable Theories*, North-Holland, 1953.

VAN HEIJENOORT, J, *From Frege to Gödel: A Source Book in Mathematical Logic 1879–1931*, Harvard University Press, 1967.

Glosario de símbolos

El número de página dada es aquel en que el símbolo ha sido o bien definido o bien usado por primera vez. No se indican los números de página para los símbolos matemáticos standard de uso frecuente. Los símbolos se han agrupado como sigue: letras castellanas, letras griegas, símbolos matemáticos, símbolos lógicos.

a_i	constante individual
$\bar{a}_i$	interpretación de constante individual
$A, B, C, \ldots$	letras de enunciado
A_i^n	letra de predicado
$\bar{A}_i^n$	interpretaciones de letras de predicado
$\hat{A}_i^n$	interpretaciones de letras de predicado
$\mathscr{A}, \mathscr{B}, \mathscr{C}, \ldots$	formas enunciativas
$\mathscr{A}, \mathscr{B}, \mathscr{C}, \ldots$	fórmulas bien formadas de L
$\mathscr{A}, \mathscr{B}, \mathscr{C}, \ldots$	fórmulas bien formadas de $\mathscr{L}$
$\mathscr{A}'$	clausura universal de $\mathscr{A}$
(AC)	axioma de elección
B	símbolo de cinta para máquina de Turing (blanco)
C_r	función característica
(CH)	hipótesis del continuo
D_I	dominio de la interpretación I
$D(m, n)$	relación en D_n
D_N	conjunto de los números naturales
$\mathscr{D}(x_1, x_2)$	fórmula bien formada de $\mathscr{N}$
D	símbolo de cinta para máquina de Turing (derecha)
Dm	relación sobre D_N
$(E7),(E8),(E9)$	axiomas
$(E7'),(E8'),(E9')$	axiomas
f_i^n	letra de función
$\bar{f}_i^n$	interpretación de letra de función
$\hat{f}_i^n$	interpretación de letra de función

fbf.	fórmula bien formada (de L)
fbf.	fórmula bien formada (de $\mathscr{L}$)
F	valor de verdad falso
$\mathscr{F}$	sistema de la teoría de cuerpos de primer orden
$\mathscr{F}_k(x_{i_k})$	fórmula de $\mathscr{L}$
$\mathscr{G}$	sistema de la teoría de grupos de primer orden
$\mathscr{G}_k$	fórmula de $\mathscr{L}$
$(G1),(G2),(G3)$	axiomas
I	interpretación
I	símbolo de cinta para máquina de Turing (izquierda)
$\mathscr{I}$	fórmula de $\mathscr{N}$
J	extensión completa consistente de L
K	sistema de cálculo de predicados de primer orden
K	conjunto asociado a una lista de máquinas de Turing
$K_{\mathscr{L}}$	sistema de cálculo de predicados de primer orden
$(K1)$, ..., $(K6)$	axiomas
$K_{\mathscr{L}N}$	sistema de cálculo de predicados de primer orden con el lenguaje de la aritmética
L	sistema de cálculo de enunciados
$(L1),(L2),(L3)$	axiomas
$\mathscr{L}$	lenguaje de primer orden
$\mathscr{L}_G$	lenguaje de primer orden de la teoría de grupos
$\mathscr{L}_N$	lenguaje de primer orden de la aritmética
MP	regla de deducción (para L)
MP	regla de deducción (para K)
N	interpretación aritmética
$(N1)$, ..., $(N7)$	axiomas
$(N1^*)$, ..., $(N7^*)$	axiomas
$\mathscr{N}$	sistema de primer orden de la aritmética
p_1, p_2, p_3, ...	símbolos de L
p, q, r, ...	variables de enunciado
p_i	i-ésimo número primo impar

p_i^k	función proyección
$Prax$	relación sobre D_N
$Prax_s$	relación sobre D_N
$\mathscr{P}(x_1, x_2)$	fórmula de $\mathscr{N}$
$q_0, q_1, q_2, \ldots$	estados internos de máquina de Turing
Q_j	cuantificador arbitrario
Q_j^*	cuantificador arbitrario
Q_{ij}	variable de enunciado o su negación
rs_2	resto de dividir por 2
$R, S, \ldots$	relaciones arbitrarias sobre D_N
$\bar{R}$	complementaria de R
s	función sucesor
sg	función sobre D_N
$\bar{sg}$	función sobre D_N
S_A	conjunto de palabras del alfabeto A
S_A^*	conjunto de clases de equivalencia de palabras
$S(I)$	sistema de primer orden del modelo I
$\mathscr{S}$	sistema de primer orden de la teoría de semigrupos
SH	regla de deducción (para L)
SH	regla de deducción (para $\mathscr{L}$)
T	extensión completa consistente de K
$T_0, T_1, T_2, \ldots$	enumeración de máquinas de Turing
$T(n)$	relación sobre D_N
$\mathscr{T}(x_1)$	fórmula de $\mathscr{N}$
V	valor de verdad verdadero
$v(\mathscr{A})$	valor de verdad de la fórmula $\mathscr{A}$
$v(x_i)$	valoración de la variable x_i
$v(t)$	valoración del término t
$W(m, n)$	relación sobre D_N
$\mathscr{W}(x_1, x_2)$	fórmula de $\mathscr{N}$
x_i	variable en $\mathscr{L}$
x'	sucesor de x
$\{x\}$	conjunto unitario
$[x]$	clase de equivalencia que contiene a x
$\{x_1, x_2\}$	par no ordenado
$z(n)$	función cero
$Z(m, n)$	función cero
ZF	sistema formal de teoría de conjuntos
$(ZF_1), \ldots, (ZF8)$	axiomas

$\mathbb{Z}$	conjunto de los enteros
$\in$	pertenencia entre conjuntos
μ	operador de minimización
Π_n-forma	forma prenexa
Σ_n-forma	forma prenexa
$\varphi_0, \varphi_1, \varphi_2, \ldots$	enumeración de las funciones parciales recursivas
$>$	vuelta a la exposición principal después de haberla interrumpido por una proposición, ejemplo, observación, corolario o definición
ϕ	conjunto vacío
$\circ$	composición de funciones
$\dot{-}$	sustracción modificada
$'$	sucesor
$\wedge$	conjunción
$\wedge$	conjunción en $\mathscr{L}$
$\vee$	disyunción
$\vee$	disyunción en $\mathscr{L}$
$\sim$	negación
$\rightarrow$	condicional
$\leftrightarrow$	bicondicional
$\leftrightarrow$	bicondicional en $\mathscr{L}$
$\downarrow$	nor
$\mid$	nand
$\bigwedge_{i=1}^{n}$	conjunción
$\bigvee_{i=1}^{u}$	disyunción
$\vdash_L$	derivación en L
$\vdash_K$	derivación en K
$\models$	verdad en una interpretación
$\forall$	cuantificador universal
$\exists$	cuantificador existencial
$\exists$	cuantificador existencial en $\mathscr{L}$
$\exists_1$	cuantificador existencial modificado
$0^{(n)}$	término en $\mathscr{N}$

Indice alfabético de materias

alfabeto de símbolos, 61
  para la lógica de primer orden, 179
  para una máquina de Turing, 169
algoritmo, 169-170
  computable mediante, 169-170
alternaciones de cuantificadores, 102
anillos, sistema de primer orden para, 126-127
apareamiento, axioma de, 133-134
argumentación, 31-35
aritmética
  indecidibilidad recursiva, 207
  interpretación standard, 69
  lenguaje de primer orden para la, 63
  sistema de primer orden de la, 128-132
  sistema de segundo orden de la, 167
axioma(s), 38
  del conjunto potencia, 134
  del conjunto vacío, 133
  de elección, 136
  lógicos, 117
  para *K*, 84
  para *L*, 38
  para la aritmética, 128
  para la igualdad, 118
  para la teoría de conjuntos, 133-134
    para la teoría de grupos, 123
  propios, 117, 167

básica
  conjunción, 25
  función, 149
bicondicional, 15
  como símbolo definido de $\mathscr{L}$, 92

cálculo
  de enunciados formal, 37-55
  de enunciados informal, 9-36
  de predicados, 67, 84-115
  de predicados puro, 207

cerrado
  fbf. (fórmula bien formada), 78, 79
  término, 108
cierre universal, 94-118
cinta de máquina de Turing, 178-179
  descripción instantánea de, 189, 200
Cohen, P. J., 137
completo(a)
  extensión de *L*, 50
  sistema de primer orden, 104
composición de funciones, 149
computabilidad, 169-177
computable
  mediante algoritmo, 171-172
  mediante máquina de Turing, 191
computadora abstracta, 171
condicional, 14
conectiva, 9-11
conjunción, 12-13, 23
  básica, 25
  como símbolo definido de $\mathscr{L}$, 64
conjunto
  no numerable, 216
  numerable, 214
  potencia, 134
  unitario, 155
  vacío, 133, 154
conjunto adecuado de conectivas, 28-31
  consecuencia
    directa, 38
    en *K*, 85
    en *L*, 40
  consistencia
    de *K*, 87
    de *L*, 49
    relativa, 138
    ω-consistencia, 164
    y modelos, 138-139
  consistente
    extensión consistente de *L*, 49

sistema de primer orden consistente, 103
constante individual, 62
contradicción
en el cálculo de enunciados informal, 17
demostración por, 35
contradictorio, 80
cuádruplas para una máquina de Turing, 180
cuantificador
existencial, 58
existencial como símbolo definido de, 65
de existencia única, 122
universal, 58
cuerpos, sistema de primer orden para los, 127-128
Church, tesis de, 172

decidibilidad de *L*, 54
decidible, recursivamente, 204-205
deducción
en *K*, 85
en *L*, 39
demostrablemente equivalentes, 92
demostración
por contradicción, 35
por inducción, 22
en *K*, 85
en *L*, 39
descripción instantánea de una máquina de Turing, 189, 200
desigualdad en $\mathcal{N}$, 142-144
disyunción, 13, 23
como símbolo definido de $\mathcal{L}$, 65
dominio de una interpretación, 68

ecuación diofántica, 170
efectivamente enumerable, 175
elección, axioma de, 136
enunciado
compuesto, 10
simple, 10
equivalencia
bicondicional, 15
bicondicional como símbolo definido de $\mathcal{L}$, 92
de palabras, 199
demostrable, 92
lógica, 18
esquema de axioma, 38, 85
estado interno de una máquina de Turing, 179
expresabilidad en $\mathcal{N}$, 142-148
extensión
de *K*, 103
de *L*, 48
finita, 209
extensionabilidad, axioma de, 133

falsedad en una interpretación, 75
finitamente presentado
grupo, 203
semigrupo, 199
forma argumentativa, 32
inválida, 32
válida, 32
forma enunciativa, 11, 15
restringida, 22
forma normal
conjuntiva, 27
disyuntiva, 26
prenexa, 97-102
formal
aritmética formal, 128-132
sistema deductivo formal, 37-38
teoría de conjuntos formal, 132-137
fórmula
atómica, 64
bien formada, en *L*, 38
bien formada, en $\mathcal{L}$, 65
cerrada, 79, 80
Fraenkel, A., 133
función
básica, 149
característica, 152
cero, 147-149
computable mediante algoritmo, 171
constante, 152
parcial, 150
parcial recursiva, 171
proyección, de, 149
recursiva, 151
fundamento, axioma de, 135
generalización, 85

Gödel, K., 110, 132, 136, 137, 140
grupos
indecidibilidad recursiva, 211
lenguaje de primer orden para los, 63
problema de palabras para, 204
sistema de primer orden de, 123-128
grupos abelianos
decidibilidad recursiva, 211
problema de palabras, 204

Hilbert, Décimo Problema de, 169
hipótesis, al usar el teorema de deducción, 44
hipótesis del continuo, 136

i-equivalentes, 72
igualdad, axiomas para la, 118
implicación
condicional, 14
lógica, 18

incompletitud de la aritmética, 131-132, 140-168
inconsistente, 49-50
indecidibilidad de sistemas formales, 204-212
independencia de (*AC*) y (*CH*), 137
inducción
  demostración por, 22
  matemática, 130
  principio de, 130
infinitud, axioma de, 134
interpretación, 68-71
  dominio de, 68
  falsedad en, 75
  verdad en, 71, 75

lenguaje de primer orden, 61-68, 69
  para la aritmética, 64
  para la teoría de conjuntos, 133
  para la teoría de grupos, 64
letra
  de función, 62, 63
  de predicado, 62, 63
leyes de De Morgan, 24
libre para x_i, 67
lógicamente válido, 80
lógico(a)
  axioma, 117
  equivalencia, 18
  implicación, 18
longitud de una *fbf*., 74

máquina
  computadora abstracta, 171
  de Turing, 171, 178-196
metateorema, 41
modelo, 111-115
  no standard de $\mathcal{N}$, 132
  normal, 122
modus ponens, 38, 85

nand, 30
negación, 12
no, 12
nor, 29
número de Gödel, 140, 158-162

o, 13
operador de minimización, 150

par no ordenado, 134
palabra(s), 198
  equivalencia de, 199
  vacía, 199
parada (terminación de un cómputo), 181
  problema de parada, 194
paréntesis, convenios para su omisión, 21, 42, 65
Peano, postulados de, 129
predicado(s)
  cálculo de, 67, 84-115
  cálculo de predicados puro, 207
  letra de, 62
principio de buena ordenación, 136
problema de palabras, 198-204
  para grupos abelianos, 204
  para grupos, 204
  para semigrupos, 200
proposición, 41

radio de acción de un cuantificador, 66
realización, 38, 77
recursión, 150-151
recursivamente
  decidible (sistema), 204-205, 211
  enumerable (conjunto), 175
  indecidible (sistema), 176, 205, 211
  insoluble, 176
  resoluble (problema de palabras), 199
recursivo(a)
  conjunto, 154
  función, 151
  función parcial, 171
  función recursiva primitiva, 151
  relación, 153
reducibilidad, 197
reductio ad absurdum, 35
reemplazamiento, axioma de, 134
reflexiva, 120
regla de deducción, 38
  en *K*, 84-85
  en *L*, 38
relación
  de equivalencia, 120
  de orden en, 144, 153
expresable en $\mathcal{N}$, 144
  que está en la presentación de un grupo o semigrupo, 199
  recursiva, 153
representable en $\mathcal{N}$, 145

satisfacción, 72-73
segundo orden
  lenguaje, 69
  sistema de aritmética, 167
semigrupo, 128
  finitamente presentado, 199
  problema de palabras para, 199
silogismo hipotético
  en *K*, 89
  en *L*, 45
símbolo definido, 44, 92, 122

simétrico, 120
sistema de primer orden
  con igualdad, 117-122
  de la aritmética, 128-129
  de la teoría de conjuntos, 132-137
  de la teoría de grupos, 123-127
Skolem, paradoja de, 139
sustitución
  en *fbf.* de $\mathscr{L}$, 92-96
  reglas para la, 19-23

tabla de verdad, 12-19
tautología
  en el cálculo de enunciados informal, 17
  en *L*, 48
  en un lenguaje de primer orden, 77
teorema, 41
  de *K*, 85
  de *L*, 39
  de adecuación para *K*, 103, 110
  de adecuación para *L*, 53
  de compacidad, 114
  de completitud (de adecuación) para *K*, 103, 110
  de completitud (de adecuación) para *L*, 53
  de corrección para *K*, 87
  de corrección para *L*, 48
  de deducción para *K*, 88
  de deducción para *L*, 43
  de deducción (recíproco) para *K*, 89
  de deducción (recíproco) para *L*, 44
  de enumeración, 190
  de incompletitud de Gödel, 140-168
    enunciado del mismo, 165
  de *K*, 85
  de *L*, 39
  de Löwenheim-Skolem, 113
teoría de conjuntos, sistema formal de, 132-137
término, 64
  cerrado, 108
  numeral, 143
Thue, sistema de, 171
transitiva, 120
Turing, A. M., 171
  tesis de Turing, 192
  máquina de Turing, 171, 178-197
  máquina de Turing universal, 193

uniones, axioma de las, 134

vacío(a)
  conjunto, 133, 155
  palabra, 199
variable
  cambio de variable ligada, 66-67, 94
  de enunciado, 11
  libre, 66
  ligada, 58, 66
válida
  fbf. lógicamente válida, 80
  forma argumentativa válida, 32
valoración
  en *L*, 47
  en una interpretación, 72
valor de verdad, 11
verdad
  en una interpretación, 70-71, 75
  función de, 12-19
  tabla de, 12-19
  valor de, 11

ω-consistencia, 165

y, 12

Zermelo-Fraenkel, teoría de conjuntos de, 132-137
Zorn, lema de, 136

COLECCION "LOGICA Y TEORIA DE LA CIENCIA"

ALWOOD, ANDERSSON y DAHL.– LOGICA PARA LINGUISTAS.– Completa introducción a la lógica para su aplicación en la lingüística y, especialmente, en la semántica. Incluye un estudio de lógica modal, lógica intensional, gramática categorial y otros temas de interés para el lingüista, además de hacer constante referencia a la relación entre lenguajes naturales y artificiales. (De próxima aparición.)

BOCHENSKI.–COMPENDIO DE LOGICA MATEMATICA.– Especialmente dirigido a estudiantes de lógica de Facultades Universitarias de Letras y Ciencias. Manual escrito por uno de los mayores especialistas en Lógica Matemática e Historia de la Lógica, incluye abundante bibliografía en inglés y español. (120 págs.– 15,5 x 21,5 cm.– Rústica.)

BOOLE.– INVESTIGACION SOBRE LAS LEYES DEL PENSAMIENTO.– La principal obra del creador de la Lógica Matemática. De interés para lógicos y matemáticos. Boole introduce en las modernas técnicas del análisis formal y realiza una amplia discusión de temas filosóficos afines. Al final estudia la teoría de probabilidades. (De próxima aparición.)

BOUDOT.– LOGICA INDUCTIVA Y PROBABILIDAD.– De gran interés para estudiantes de Lógica, Estadística y Matemáticas. Estudio detallado de las relaciones entre inducción y teoría de la probabilidad. Especial análisis de las teorías de Reichenbach y Keynes. (348 págs.– 15,5 x 21,5 cm.– Rústica.)

FEYS y FITCH.– LOS SIMBOLOS DE LA LOGICA MATEMATICA.– Unica obra en la que se presentan y comparan las distintas notaciones simbólicas de la Lógica Matemática. (192 págs.– 15,5 x 21,5 cm.– Rústica.)

GARDIES.– LOGICA DEL TIEMPO.– Completa exposición de todos los sistemas existentes de lógica temporal. Incluye una discusión de las lógicas temporales gramaticales. (128 págs.– 15,5 x 21,5 cm.– Rústica.)

HAACK.– LOGICA DIVERGENTE.– Minucioso estudio de las más recientes direcciones de la lógica y, especialmente, de las que se apartan de la Lógica ortodoxa. (192 págs.– 15,5 x x 21,5 cm.– Rústica).

HUNTER.– METALOGICA. INTRODUCCION A LA METATEORIA DE LA LOGICA CLASICA DE PRIMER ORDEN.– El primer manual completo en castellano sobre este tema. De interés para los estudiosos de la Lógica, las Matemáticas y la Teoría de la Computación. Nociones básicas para el examen de los sistemas lógicos, estudio detallado de las propiedades de los mismos y teoremas anejos. (De próxima aparición.)

MARTINEZ FREIRE.– FILOSOFIA DE LA CIENCIA EMPIRICA.– Investigación exhaustiva de los principales temas de la Ciencia Empírica y de la Lógica Inductiva, siguiendo las doctrinas de Whewell. (232 págs.– 15,5 x 21,5 cm.– Rústica.)

THIBAUD.– LA LOGICA DE CHARLES SANDERS PEIRCE.– Estudio sucinto y esencial de la obra de Peirce, lógico americano muy valorado en la actualidad y fundador de la lógica de relaciones. Aspectos algebraicos y gráficos típicos de Peirce e importantes temas de la lógica modal. De interés para estudiantes y profesores de lógica. (De próxima aparición.)

WHITEHEAD y RUSSELL.– PRINCIPIA MATHEMATICA.– La obra clásica de la Lógica Matemática. Estudio completo de los fundamentos de la misma que permite iniciarse al lector en los tópicos básicos de la filosofía de la matemática. Sostiene la fundamentación de las Matemáticas desde la Lógica. (De próxima aparición.)

PUBLICADOS POR PARANINFO S.A.

EDITORIAL
PARANINFO S.A.
Magallanes, 25.—Madrid-15.